Authentication Guide for Europe

Version 1.3

26 March 2020

ATNGE

Contents

Chapter 1 Naming Convention

In this document, the following naming convention is used to refer to flags/indicators in authentication, authorization and clearing messages.

Authentication

All authentication fields are highlighted in italic and underlined.

Authorization (fields starting with DE)

Reference	DE	Data Element Name
Transaction Amount	DE 04	DE 4—Transaction Amount
POS Entry Mode	DE 22	DE 22—Point-of-Service (POS) Entry Mode
DE32	DE 32	DE 32—Acquiring Institution ID Code
RC	DE 39	DE 39—Response Code
Merchant name	DE 43	DE 43—Card Acceptor Name/Location for ATM Transactions
SLI	DE 48 SE 42 SF 1	DE 48 (Additional Data—Private Use), sub-element 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator)
AAV	DE 48 SE 43	DE 48 (Additional Data), subelement 43 (UCAF)
Trace ID	DE 48 SE 63	DE 48 (Additional Data), subelement 63 (Trace ID)
Program Protocol	DE 48 SE 66 SF 1	DE 48 (Additional Data), subelement 66 (Authentication Data), sub-field 1 (Program Protocol)
DS Transaction ID	DE 48 SE 66 SF2	DE 48 (Additional Data), subelement 66 (Authentication Data), sub-field 2 (Directory Server Transaction ID)
	DE 61 SF 4	DE 61 (POS Data), subfield 4 (POS Cardholder Presence).
	DE 63 SF 1	DE 63 (Network Data), subfield 1 (Financial Network Code)

Clearing (Fields starting with "PDS")

Reference	DE	Data Element Name
SLI	PDS0052	Electronic Commerce Security Level Indicator
DS Transaction ID	PDS0184	Directory Server Transaction ID
Program Protocol	PDS0186	Program Protocol

Chapter 2 General Authentication Requirement

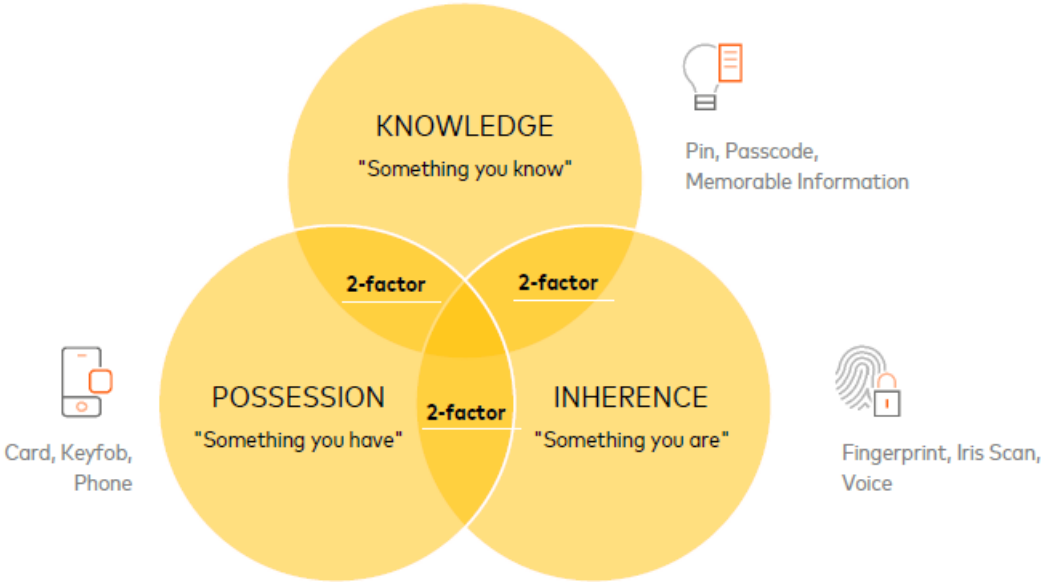
This section provides information on general authentication requirements for Europe.

Strong Customer Authentication (SCA)

Strong Customer Authentication (SCA) can be performed using two-factor authentication.

For example, two of the following three factors have to be systematically used during the authentication experience:

- Knowledge—something only the Cardholder knows: password, PIN
- Possession—something only the Cardholder has: mobile phone
- Inherence—something the Cardholder is: finger, face, voice, behavioral biometrics



Mastercard has developed the Mastercard Identity Check™ Program to support stronger authentication methods and ban at the same time methods that **alone** (for example, not combined with other methods such as SMS OTP) have proved to be too weak: static passwords, security questions, Knowledge-Based Authentication or KBA.

For more information on banned authentication methods as well as recommended authentication methods (such as, biometry, Risk-Based Authentication/RBA), refer to *Mastercard Identity Check™ Program Guide (19 November 2019)*.

Most common SCA mechanisms in the Europe Region and as per research include:

- **Biometry** (fingerprint, facial recognition) on consumer devices (such as, mobile phones), and sometimes PIN on consumer devices.
  - Mastercard strongly recommends that Issuers roll-out authentication or mobile banking apps with biometrics by April 2019 unless other specific dates have been defined for their country (refer to Appendix A for the list of those countries) to meet the Mastercard biometric mandate.

- **One-time password** (OTP) sent via SMS when allowed by national competent authorities. This authentication method is considered as a valid solution as per the *Mastercard Identity Check™ Program Guide* (19 November 2019).
  SMS OTP is a one-factor (possession of the SIM card) and combined with a knowledge factor or inherence factor (such as, a security question, a PIN code, or behavioral biometrics) qualifies as SCA meeting PSD2 requirements in some markets. In some other markets (such as, United Kingdom), SMS OTP with card data meets the requirements of the national competent authorities (NCAs). When adding a knowledge factor to the SMS OTP, a security question works better (lower abandonment rate) than a PIN. Both are deemed two-factor authentication compliant with the EBA opinion.

  SMS OTP is defined as an acceptable alternative to biometry in the Mastercard Identity Check™ Program.

Mastercard highly recommends to replace SMS OTP with a mobile device based authentication solution. However, should SMS OTP still be one of the supported authentication methods, Mastercard recommends the following options to add a second factor to SMS OTP solutions (which use possession as the first factor, for example, the OTP confirms that the Cardholder is in possession of the mobile device to which the SMS was sent):

1. Behavioral biometrics[1] provided that these comply with PSD2 RTS' requirement that the probability is low that a non-authorized user is authenticated; behavioral biometrics are explicitly allowed as an authentication factor in the PSD2 RTS and the EBA Opinion.
2. Although concerns may be raised on transaction speed and consumer experience, Security questions, for example from a list of multiple questions; it is recommended that banks re-use existing security questions and answers used for other services (such as, call center authentications) when available or information they already have that only the Cardholder knows.
3. PIN code, but this is the least recommended option as static passcodes are likely to be forgotten. An electronic PIN (ePIN) related to remote electronic/e-commerce transactions should be used and not the real card PIN.

Strong customer authentication should be designed to offer an ideal consumer experience while optimally securing payments.

Authentication versus Authorization Amount Policy

Where possible, the authentication amount should be equal to the authorization amount. This may require whenever possible to delay the authentication until the final transaction amount is known.

To reduce fraud and to comply with PSD2 RTS' Dynamic Linking requirements (refer to section Dynamic Linking Requirements and AAV Validation), Merchants are recommended to authenticate for an amount equal or greater than the total transaction amount.

[1] Behavioral biometrics: field related to the measure of patterns in a human behavior or activities that allow to uniquely identify that human. It includes keystroke dynamics, mouse dynamics and signature analysis.

Mastercard's Position for Europe

The authentication amount for a Remote Electronic Transaction must be an amount that the cardholder would reasonably expect and the authentication must use the same currency as the authorization.

As a best practice, the total transaction amount of all authorizations that relate to an intra-EEA remote electronic transaction should not exceed the authentication amount for the transaction by more than 20 percent. If the transaction amount is not known in advance, the authentication amount must be an amount that the cardholder would reasonably expect (for example, within a tolerance of 20 percent). In this case, if the authorization amount exceeds the authenticated amount by more than 20 percent, it is recommended that merchants treat the incremental amount compared to the authenticated amount as a separate transaction. Transactions subject to PSD2 RTS may require a separate strong customer authentication unless an exemption applies or unless they are handled as Merchant Initiated Transactions (MIT). If the transaction amount exceeds the cardholder's "reasonable expectations," the refund right for authorized transactions under Articles 76-77 PSD2 may apply.

This recommendation applies to one-off payment transactions, not for adding a card to card-on-file or for initiating recurring payments.

As a single authentication may result in multiple authorizations (such as, travel bookings combining for example hotel and flight, market place purchases where items are ordered from multiple Merchants), Issuers must ensure that the total (possibly accumulated) transaction amount, for example the sum of the individual authorizations, does not exceed the authenticated amount.

Also in this case, if the transaction amount is not known in advance, the authentication amount must be an amount that the Cardholder would reasonably expect (recommended 20 percent tolerance in Europe).

As delays may be experienced between the authentication and the final authorization, the authentication code (called Accountholder Authentication Value or AAV) has to remain valid till the final authorization.

Accountholder Authentication Value (AAV) Validity and Extension

In the current Mastercard rules, there is no limit on the validity of an AAV. It should be valid for at least 90 days. Some Issuers may be able to validate an AAV older than 90 days, which is why a Merchant could try to use an AAV for more than 90 days. If an authorization with a potentially expired AAV (for example, more than 90 days old) is declined, the Merchant could re-send the authorization without the AAV and UCAF data but the merchant becomes liable in case of fraud (lost of liability shift).

Many issuers use the Mastercard On-Behalf AAV Validation Service, which are valid for 10 calendar days, except for several card acceptor business codes (MCCs) where AAVs are valid for 90 calendar days.

This list of MCCs includes 1500, 3000, 3001, 3006, 3007, 3009, 3010, 3016, 3017, 3022, 3025, 3026, 3028, 3029, 3034, 3042, 3047, 3048, 3050, 3051, 3052,3068, 3069, 3075, 3077, 3078, 3082, 3084, 3100, 3136, 3146, 3161, 3180, 3182, 3223, 3236, 3248, 3256, 3261, 3294, 3295, 3301,4111, 4112, 4121, 4722, 4789, 5732, 5735, and 7011.

The list of MCCs will vary based on customer input or Mastercard monitoring (such as high decline rates for new specific MCCs). This list will be included in the next version of the *Mastercard Identity Check Program Guide*. Refer to the following document for more information on this topic: *AN 3440—Mastercard AAV Validation Update for Merchant Category Codes*.

If the first payment authorization cannot be sent within these time frames (10 calendar days or 90 calendar days for the MCCs listed previously), then merchants must use an ASI (refer to the section on Usage of Account Status Inquiry [ASI]) with the 3DS data right after SCA. The Trace ID of this ASI should be referenced in future related authorization messages.

Issuers that do not use the Mastercard On-Behalf AAV Validation Service and self-validate AAVs should ensure that these can be validated during 90 calendar days.

After the AAV validity period, Mastercard expects that the issuer approval rates will be lower.

An extension to the AAV validity period can be requested as follows:

- Renew the AAV by using the 3RI-PA mechanism available with EMV 3DS 2.2.
- When one-authorization-multiple-clearing model is used, the Merchant can extend the authorization and refer to the original authorization using the Trace ID of this latter.

NOTE: For recurring transactions/MITs, the AAV check is not performed for subsequent transactions. Refer to the section Recurring Payments.

In case of the agent model (see section Agent Model) where a single authentication is linked to multiple authorizations, the same authentication code/AAV as per PSD2 RTS could be used for multiple transactions.

3D Servers are allowed to store the AAV until the transaction is considered as completed, for example, until the transaction has been authorized and cleared. Acquirers are reminded that valid AAVs for authenticated transactions have to be provided in clearing records in PDS 0185 (Accountholder Authentication Value - AAV) as stated in *AN 2401—Data Integrity Monitoring Program—New Edits for EMV 3-D Secure and New Alerts and Notifications Feature*.

Issuer Authentication Value

The Issuer Authentication Value (IAV) is pertinent to Issuers who perform self-validation. It is included in the Accountholder Authentication Value (AAV) in the authorization message that is generated using the Secure Payment Application (SPA) number 2 (SPA2).

Mastercard only validates the Mastercard portion of the SPA2 AAV (or any AAV) only when the Issuer enrolls the card range for the OBS 05 service through their regional CIS team for the

OBS service in MPS. Mastercard will not validate the IAV part of the SPA2 AAV. SPA1 key share is currently required. Once enrolled, all transactions with AAVs are validated.

Refer to the following document for more information on this topic: *SPA2 AAV for the Mastercard Identity Check Program*.

DS Transaction ID

The Directory Server (DS) Transaction ID will be the universal transaction identifier used to map authentications to authorizations.

This is a mandatory element in EMV 3DS specifications, Mastercard authorization's *Customer Interface Specifications* (CIS) and Mastercard Clearing's Integrated Product Messages (IPM) specifications as from 6 November 2018.

EMV 3DS	dsTransID
CIS	DE 48 SE 66 SF 2
IPM	PDS 0184

As this identifier allows the mapping of authentication, authorization and clearing transactions, it is a critical element that should be managed carefully.

Merchants/Acquirers must provide the DS Transaction ID in authorization and clearing messages.

Refer to the following document for more information on this topic: *AN 1630 - AAV Verification Service Enhancement*.

If the DS transaction ID is not provided in authorization or clearing message, transactions should not be systematically blocked. The mapping can still be done using systemic reconciliation processes.

Program Protocol

The Program Protocol is the version of the 3DS specifications being supported: 1 for 3D Secure Version 1.0 (3DS 1.0), and 2 for EMV 3-D Secure (EMV 3DS, aka 3DS 2.x).

This is a mandatory element in Mastercard authorization's CIS and Mastercard clearing's IPM specifications as from 6 November 2018:

CIS	DE 48 SE 66 SF 1
IPM	PDS 0186

Refer to the following document for more information on this topic: *AN 1630 - AAV Verification Service Enhancement*.

Merchant Names

With the clarification by the EBA on 20 December 2019 that the dynamic linking requirement is met if the Merchant is identified through its IBAN or another "unique identifier", it is not necessary that the authentication code for remote transactions is linked to the Merchant name, as initially suggested by a strict interpretation of the PSD2 SCA regulation. As a consequence of this, Issuers must not decline authorizations only because the Merchant name does not match in authentication and authorization.

Refer to section Dynamic Linking Requirements and AAV Validation for more information.

The Merchant names are captured as follows:

EMV 3DS	MerchantName
CIS	DE 43

Mastercard's Position for Europe

The following additional rule applies to intra-EEA Transactions. Effective 1 July 2020, acquirers must ensure that their online merchants always use the same merchant name in the authentication message.

NOTE: Refer to *Mastercard Rules* for the latest information on this topic. During soft enforcement of the PSD2 SCA regulation, temporary non compliance that this latter regulation is tolerated if a migration plan has been approved by the National Competent Authorities until the applicable grace period ends.

The merchant name in authentications must uniquely identify the merchant in all countries where it operates and for all its activities (for example, Merchant.com) or per its activities (such as, MerchantBooks.com, MerchantMusic.com) or per its countries (such as, Merchant.fr, Merchant.co.uk). Acquirers must ensure that the merchant name used by the merchant actually belongs to the merchant and is registered for using the Identity Check Program.

Mastercard recommends that acquirers use the same merchant name in authentication and authorization for consistency and compliance monitoring of merchant's usage of the acquirer TRA exemption. For payment facilitators, the merchant name used in authentication must mirror the one in authorizations, such as "Payment Facilitator * Submerchant".

Acquirers in the EEA must register the merchant name used in EMV 3DS authentication messages in the Identity Solutions Services Management (ISSM) tool.

Submerchants behind Payment Facilitators do not need to be registered if the Payment Facilitator is registered in ISSM (in the format "Payment Facilitator *"), but this means that ISSM flags and fields for services like merchant white listing, Authentication Express, and acquirer TRA exemptions does not work at the submerchant level. As of 1 February 2020, acquirers in the EEA must register the country code for merchants using EMV 3DS authentication messages in the Identity Solutions Services Management (ISSM) tool.

Effective May 2020, Mastercard will provide Acquirers, Issuers and their ACS's with a table listing Merchant names and Whitelisting Merchant names. This will allow:

- Merchant Whitelisting (refer to section on Merchant Whitelisting) via Issuer online banking or ACS (Access Control Server) portal. It would allow Issuers that want to offer whitelisting in their online banking services to show Merchant names as used during the authentication experience and to pass it on to the ACS which manages the Whitelisting and stores the card number/Whitelisting Merchant names. During the initial setup of Merchants on the Mastercard Directory Server via the ISSM tool on MastercardConnect.com, each Merchant with its Merchant Name can be associated to a Whitelisting Merchant Name to allow multiple Merchant names to be grouped together for whitelisting (for example, one of these Merchant Names being whitelisted will result in all the Merchant Names under that Whitelisting Merchant Name to be exempt from SCA). The Whitelisting Merchant Name will be available in ISSM on 26 March 2020.
- Acquirers and Merchants to ensure that their Merchant names are unique and consistent.

The Merchant names table will be used for whitelisting (Whitelisting Merchant Name), as well as to comply with our Merchant name rules (for example, check if a Merchant name already exists).

Acquirers should ensure they comply with GDPR, which means that their Merchants should be informed that their name will be shared with other Acquirers and Issuers.

Biometric Authentication Support

Issuers are mandated to offer Cardholders biometric authentication in most European countries as of 1 April 2019 unless other specific dates have been defined for their country (refer to Appendix A for the list of those countries).

The reference announcement specifying the mandate or recommendation and mentioning the mandate effective date is provided in Appendix B.

Refer to the following document for more information on this topic: *Mastercard Biometric Authentication—Europe Region* (11 January 2018)

Non-payment Authentications for Card Add

Non-payment authentications for Card Add always require step-up authentication, which means that Risk Based Authentication should be turned off for non-payment authentications. A step-up authentication is a strong authentication decided by the Issuer.

This is useful when SCA is required, for example to add a card to Card-On-File (COF) under PSD2 RTS. It's mandatory to use SCA for all new Cards added to COF. Provisioning qualifies as an "action through a remote channel, which may imply a risk of payment fraud or other abuses" pursuant to article 97(1) (C) PSD2. No exemptions are provided for these actions. Refer to the section on PSD2 SCA Exemptions and Exclusions.

Card details stored on file change (for any of the elements such as the card expiry date, even if the primary account number remains unchanged) require a new SCA. A new SCA is not needed when card details are changed using the Mastercard Automatic Billing Updater (ABU). In general terms, the update of card credentials (including PANs)/tokens via ABU and the Mastercard Digital Enablement Service (MDES) are PSD2 compliant. The end consumer should not go through SCA again if ABU or MDES has been used.

Mastercard recommends that after the SCA has been performed you send an Account Status Inquiry (ASI in authorization to check the associated account, except when the Card Add is done with payment (see next paragraph).

When a card is added to Card-On-File and a payment is requested in the same cardholder–merchant session (for example, cardholder does not leave merchant website or app during Add Card and payments, both of which typically happen within minutes) at the same time, only one SCA is needed to cover both the payment and the Add Card. Such a mechanism to avoid double SCA can be implemented either by the merchant in its cardholder check out flow, or by the issuer's ACS by recognizing that both EMV 3DS authentication requests (assuming the merchant sends an authentication request first for Add Card and then for payment) refer to the same cardholder–merchant session of which the second authentication request does not need SCA.

Different use cases apply as follows:

Use Case	Message Category	Requestor Challenge Indicator	Requestor Authentication Indicator	Cardholder Account Age Indicator	Purchase Amount
Add CoF without a payment	Non-Payment 02-NPA	"03" (Challenge Requested: 3DS Requestor Preference) OR "04" (Challenge Requested: Mandate) for regulated markets	"04" (Add Card)	N/A	0
Add CoF as part of a payment	Payment 01-PA				>0
Add CoF as part of the first recurring or installment	Payment 01-PA		"02" (Recurring transaction) OR "03" (Installment transaction)	"02" (During this transaction)	>0

Liability Shift with EMV 3DS

A liability shift for EMV 3DS applies effective October 2019. EMV 3DS and the Mastercard Identity Check™ Program are mandated effective 1 April 2019 unless other specific dates have been defined for the country (refer to Appendix A for the list of those countries).

The liability shift applies to 3DS independently of the program protocol version (3DS 1.0 or EMV 3DS). If the Merchant does not support 3DS or uses Identity Check Insights (refer to section Acquirer SCA Exemptions), liability in case of fraud is with the Acquirer/Merchant. In all other cases, the Issuer is liable if no Acquirer PSD2 SCA exemption applies or if the Issuer has delegated SCA to the Merchant. Refer to section on PSD2 SCA Exemptions and Exclusions.

If the Merchant applies an Acquirer exemption through 3DS and the Issuer accepts it (SLI 216), then the Merchant is liable. If the Issuer goes through SCA without accepting an Acquirer exemption (SLI 212), the Issuer is liable.

	Cells driving liablitity				Cells where liability changes from default
Exemption/Exclusion	**Transaction submitted via 3DS**	**Exemption applied by Acquirer**	**Exemption applied by Issuer**	**Issuer Challenge**	**Liability**
All below	No-3DS	**See below**			Acquirer
No	X				Issuer (default)
All exclusions except subsequent MITs	X	**Exclusion**			Issuer (default)
Low value transactions	X	X			Acquirer
Low value transactions	X	X		X	Issuer
TRA	X	X			Acquirer
TRA	X	X		X	Issuer
SCA Delegation	X	X			Acquirer
SCA Delegation	X	X		X	Issuer
Recurring payment - First	X	X		Mandate	Issuer
Recurring payment - Subsequent	X	X			Acquirer
MIT - First	X	**Exclusion**		Mandate	Issuer
MIT - Subsequent	X	**Exclusion**			Acquirer
Low value transactions	X		X		Issuer
TRA	X		X		Issuer
Trusted Beneficiaries	X		X		Issuer
Secure Corporate Payments	X		X		Issuer

Co-existence of 3DS 1.0 and EMV 3DS

Mastercard does not envision the end of the liability shift for 3DS 1.0, and 3DS 1.0 and EMV 3DS will co-exist.

- Merchants not yet upgraded to EMV 3DS have the possibility to continue using 3DS 1.0 until the Mastercard mandates are in place. The reference announcement specifying the mandates and their effective date is provided in Appendix B.
- Issuers should not decline transactions only because 3DS 1.0 is used by the Merchant. The Issuer ACS should be capable of handling authentication requests from Merchants in both 3DS 1.0 format and EMV 3DS.
- Merchants should bear in mind that EMV 3DS allows the transport of authentication elements (such as, device insights) that will allow Issuers to ensure transaction monitoring for every remote electronic transaction.

Before the Mastercard Identity Check™ Program mandate on 1 April 2019 (unless other specific dates have been defined for their country, refer to Appendix A for the list of those countries), Merchants can only use EMV 3DS if the Issuer is enrolled in EMV 3DS. If not, a fall back to 3DS 1.0 will be needed. Merchants can check which card ranges are enrolled in EMV 3DS by sending EMV 3DS Preparation Request (PReq) messages, which the Mastercard Directory Server (DS) answers by providing enrolled card ranges in the EMV 3DS Preparation Response (PRes) messages. The information is provided in the Card Range Data.

The reference announcement specifying the mandate or recommendation and mentioning the mandate effective date is provided in Appendix B.

For Acquirers that have been mandated to support EMV 3DS as from 1 April 2019, Merchants still need to check that the Issuer is in one of the 12 countries (countries flagged as in CEE in Appendix B) mandated to support EMV 3DS on 1 September 2019. If this is the case and the Issuer has not yet migrated to EMV 3DS, Merchants need to fall back to 3DS 1.0 until 1 September 2019.

NOTE: The Merchant must not retry with 3DS 1.0 if an EMV 3DS authentication request fails with Transaction Status "N" (Not Authenticated /Account Not Verified; Transaction denied).

If an Issuer does not support EMV 3DS after the PSD2 effective date, Mastercard has implemented a stand-in authentication service (enrollment by default with opt-out option), called Smart Authentication Stand-In.

Refer to the section Authentication Services.

If the transaction is scored as low risk then the authentication will be approved up to a certain amount to be set by the Issuer (30€ by default[2]). If not (high risk transaction or amount above €30), the authentication response will indicate a Merchant attempt.

If the authentication was approved in authentication stand-in, the authorization request will indicate a fully authenticated transaction (SLI 212) however, the AAV will specify that authentication stand-in was applied (AAV will have leading indicator kJ or kC). Issuers that cannot apply a TRA or other exemptions and hence rely on low value payment exemption for such authentication stand-in transactions should ensure that the transaction counter (maximum 5) or cumulative value (maximum €100) are not exceeded since the last SCA, as per PSD2 RTS. This counter or cumulative amount validation during the authorization is also needed if the transaction uses an Acquirer exemption for low value payments (Low Transaction Risk Indicator in DE48 SE 22 SF1 = "04" (Low Value Payment) as only the Issuer can track this counter or cumulative amount as per PSD2 RTS.

If during the authorization processing the Issuer decides that SCA is required, for example because the cumulative counter or value is exceeded, then the authorization response should use response code 65 (RC65). Merchants are then required to go through 3DS authentication to enable the Issuer to apply SCA. Refer to the section Soft Decline or Decline-as-SCA-Required.

[2] In early 2020 Mastercard may enhance the service and allow Issuers to change this limit in line with their fraud rate and TRA exemption limit.

Friendly Fraud and Cardholder Challenge

Friendly fraud (the consumer conducts a transaction and then files it as false chargeback using believable reasons) is a type of fraud that will require Issuer awareness and clear guidelines and best practices for their customer support/helpdesk staff.

When friendly fraud is suspected, the Cardholder should be challenged using various techniques through his/her first line interview, including but not limited to:

- The comparison of shipment address and device insights with EMV 3DS provided data.
- (Possibly) The challenge of the location via geolocation information provided by the Merchant (such as, if Merchant app was used).
  Questions of this type should be captured in the script to be run by the Issuer's first line of support/helpdesk.

  The Mastercard Claims Manager has a collaboration layer where Issuers can communicate with Merchants directly to share insights prior to sending a formal chargeback.

General Data Privacy Regulation (GDPR)

Customers are strongly encouraged to consult with their legal counsel with regards to their GDPR compliance obligations.

Key Principles

- Legal ground: Merchants and Customers may rely on other legal basis than consent, including legal obligation (PSD2), contract and legitimate interest for disclosing personal data in the context of EMV 3DS and for performing Risk-Based Authentication (RBA) based on profiling.
- Purpose limitation: Mastercard and Issuers will not use EMV 3DS data for other purposes than fraud prevention and authentication, or as provided in Mastercard Rules. It excludes the usage of personal data for other purposes, such as sales, marketing and data mining (other than fraud prevention as purpose) activities. Merchants/Acquirers need to make sure their terms and conditions (especially their privacy notices) are amended to account for the capture of additional data.
- Transparency: Individuals must be provided with detailed information about how their data is collected, used and processed. This can be ensured via a Privacy Notice including at a minimum the types of data being processed, the purposes of their processing, and data uses.

EMV 3DS and Data Collection

EMV 3DS requires that Merchants collect much more data during the checkout experience.

Appendix D provides the list of EMV 3DS 2.1 fields that are required, conditional or optional by EMVCo and by Mastercard.

It appears that some of the mandatory EMV 3DS data is not always collected, such as the title/prefix, surname, the shipping address or the house number.

When this is the case, some dummy values or processes to copy data from other fields may be required. The following provides some guidance on these:

- Title/prefix should be "M." if not captured from the cardholder.
- House number should be extracted from the street name (included number) if not captured separately or set to a default value (such as, "99999" or similar).
- Additional address info should be space-filled if not captured.
- Shipping address should by default be equal to the billing address and vice versa, if not provided separately.

Staged Wallets

In the case of staged wallets where an initial funding transaction is followed by payment transactions, the following points are important.

- If a wallet provider provides SCA services to an Issuer, the Issuer should ensure that SCA delegation to that wallet provider has been agreed upon. Mastercard has made available a program that will facilitate SCA delegation. *AN 2714—Authentication Express—an Authentication Program Enabling Easy and Secure Multi-Lateral SCA Delegation* announces the Mastercard SCA delegation service (Authentication Express) availability.
- As Merchant-Initiated Transactions are out of scope of the PSD2 RTS on SCA for card payments, these would apply to funding transactions, which means that no SCA would be required.

Chapter 3 PSD2 SCA

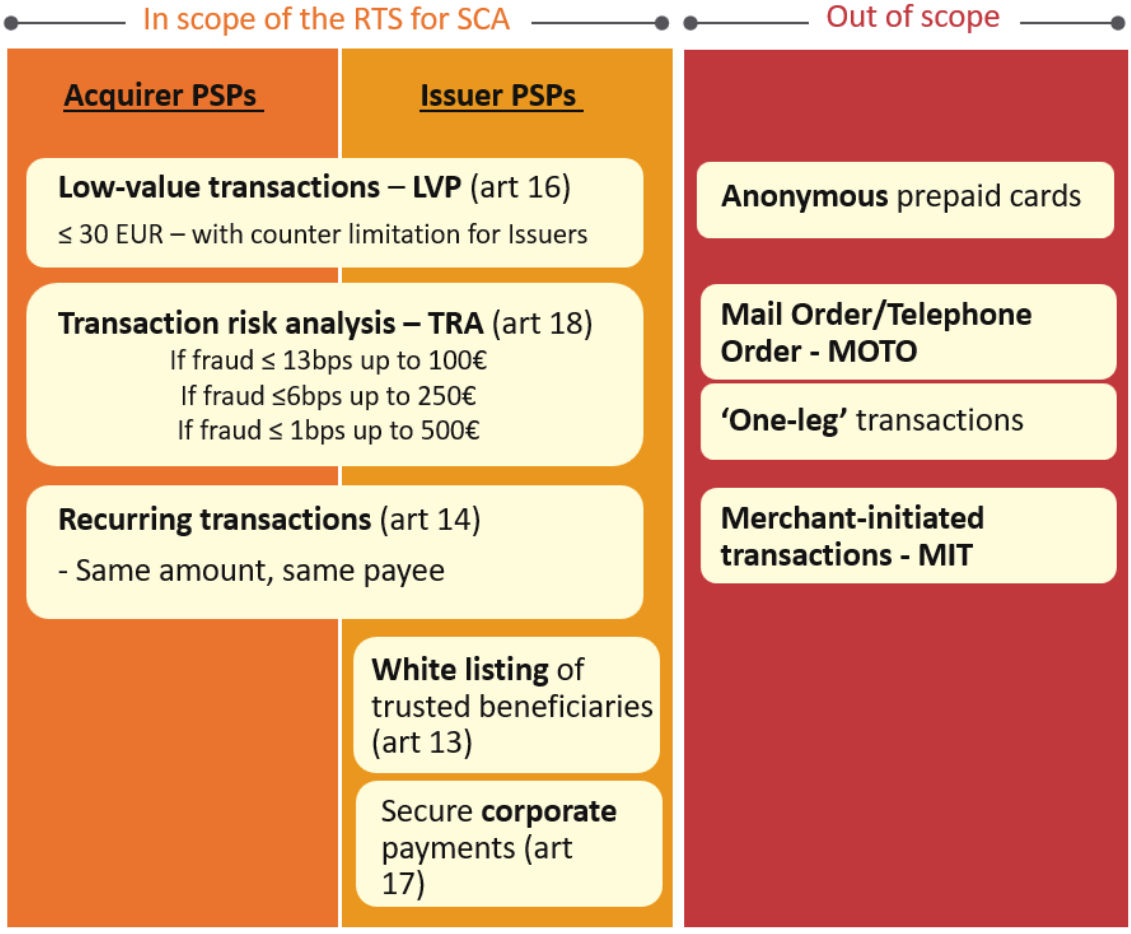
The following chapter will provide details on the applicability of each of these circumstances as well as specifics of how to recognize them and what to do when recognized.

NOTE: In this chapter and the remainder of this manual, the effective date of the PSD2 RTS on SCA (14 September 2019) is mentioned at several occasions in Mastercard's Positions for Europe on such as, Acquirer exemptions, the Acquirer country code, recurring payment transactions and grandfathering, as well as Merchant Initiated Transactions.

As per the Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 of 21 June 2019 (EBA-Op-2019-06), this effective date could be delayed when an Acquirer or Issuer has agreed on a PSD2 SCA migration plan with the National Competent Authorities. During soft enforcement, Issuers by all means should make sure that they do not decline authorizations without authentication.

PSD2 SCA Exemptions and Exclusions

An important aspect of the PSD2 RTS is the set of exemptions that will apply in various circumstances. The following diagram depicts the areas in-scope of the PSD2 RTS but exempted (left-hand side), and the areas out-of-scope of the PSD2 RTS (right-hand side).



EMV 3DS Support of the PSD2 RTS on SCA

The EMV 3DS 2.2 specifications include a set of features to support the PSD2 RTS on SCA.

- **Acquirer SCA exemptions** through the 3DS Requestor Challenge Indicator
- **Whitelisting** through the Whitelist Status
- **MOTO transactions** through the 3RI Indicator and message flow for payments (EMV 3DS 2.1 supports 3RI but only for non-payments)

This data is not available in the current EMV 3DS 2.1 specifications. As the time line for rollout of EMV 3DS 2.2 is not yet decided and there is an urgent need to provide a platform allowing compliance by the PSD2 effective date of 14 September 2019, Mastercard has defined a new Mastercard PSD2 Message Extension to the current EMV 3DS 2.1 specifications that will support some of the EMV 3DS 2.2 features listed above but also introduce new data elements that will help to support the PSD2 RTS on SCA and that are not covered by the EMV 3DS 2.1 nor the EMV 3DS 2.2. The EMV 3DS 2.1 specifications amended with the Mastercard PSD2 Message Extension is referred to as the EMV 3DS 2.1+ specifications in the remainder of this document and other publications. AReq Fields 2, 3 and 4 in the table below (merchantFraudRate, acquirerCountryCode and secureCorporatePaymentExemption) are part of a Mastercard PSD2 Message Extension in EMV 3DS 2.2 and future versions until these fields have been integrated in the EMVCo specifications at industry level.

Refer to the announcement, *AN 2758 – Announcing the New EMV 3DS 2.1 Mastercard Message Extension*.

The following is a list of those data elements.

Feature	EMV 3DS 2.1 – PSD2 Mastercard Message Extension (AN 2758—Announcing the New EMV 3DS 2.1 Mastercard Message Extension in EEA Countries)	EMV 3DS 2.2
SCA Exemption (in ARes and RReq only)	PSD2 Mastercard Message Extension **AReq Field 1 = 3DS Requestor Challenge Indicator** 05 = No challenge requested transactional risk analysis is already performed). **05 will be used for the following Acquirer exemptions: low- value payment, TRA, recurring payment AND MIT (refer to section on Merchant-Initiated Transactions)** 07 = No challenge requested (strong consumer authentication is already performed under Issuer delegation). *AN 2714—Authentication Express—an Authentication Program Enabling Easy and Secure Multi-Lateral SCA Delegation* announces the Mastercard SCA delegation service (Authentication Express) availability. For both values "05" and "07", the ARes will include a transStatus = "N" and transStatusReason = "81".	Already supported in specs Field three DS Requestor Challenge Ind = Same values as in previous column. For both values "05" and "07", the ARes will include a transStatus = "I".
Merchant Fraud Rate (in AREq only)	PSD2 Mastercard Message Extension AReq Field 2 = Merchant fraud rate in bps taking into account all Merchant sites and card volumes, calculated as per PSD2 RTS Article 19 1= fraud level <=1 bps 2= fraud level >1 and <= 6 bps 3= fraud level >6 and <= 13 bps 4= fraud level >13 and >= 25 bps 5= fraud level >25 bps The merchant fraud rate is optional and has to be calculated by the Acquirer as per PSD2 RTS (EEA volumes, remote electronic transactions excluding out of scope items (MOTO, MIT), for all schemes)	Same as in previous column

Feature	EMV 3DS 2.1 – PSD2 Mastercard Message Extension (AN 2758—Announcing the New EMV 3DS 2.1 Mastercard Message Extension in EEA Countries)	EMV 3DS 2.2
Acquirer Country Code (in AReq only)	PSD2 Mastercard Message Extension AReq Field 3 = numeric ISO country code of the Acquirer if in the EEA. If the ISO country code is in the EEA, then related transactions are in scope of the PSD2 RTS on SCA.	Same as in previous column
Secure Corporate Payment (in AReq only)	PSD2 Mastercard Message Extension AReq Field 4 = Whether the electronic payment transaction uses dedicated payment processes or protocols under PSD2 RTS Article 17's Secure Corporate Payment Exemption which the Issuer can apply Y = yes N = no	Same as in previous column
Whitelist Status (in ARes only)	PSD2 Mastercard Message Extension ARes Field 1 = Y = 3DS Requestor is whitelisted by cardholder N = 3DS Requestor is not whitelisted by cardholder E = Not eligible as determined by Issuer P = Pending confirmation by cardholder R = Cardholder rejected U = Whitelist status unknown, unavailable, or does not apply	Already supported in specs Field whiteListStatus = same values as in previous column

For the sake of completeness, please find below the HTML templates to be used for the new fields in the message extension for both Merchant Data and ACS Data:

```
"messageExtension": [{
    "name": "Merchant Data",
    "id": "A000000004-merchantData",
    "criticalityIndicator": "false",
    "data": {
        "A000000004-merchantData":{
            "scaExemptions": "05",
            "merchantFraudRate": "1" ,
            "acquirerCountryCode": "050",
            "secureCorporatePaymentExemption": "Y"
        }
    }
"messageExtension": [{
    "name": "ACS Data",
    "id": "A000000004-acsData",
    "criticalityIndicator": "false",
    "data": {
        "A000000004-acsData": {
```

```
                "whitelistStatus": "Y"
            }
        }
    }]
```

What if one of these fields is not populated in the message extension?

- NO Acquirer SCA exemption: an Acquirer exemption cannot be requested before EMV 3DS 2.2.
- NO Merchant Fraud rate: the data point is not provided to the ACS/Issuer to increase its level of confidence in the ongoing transaction. Also, Issuers may use it to decide if a Merchant should be eligible for the white listing exemption.
- NO Acquirer Country Code: an ACS/Issuer could incorrectly flag the ongoing transaction as a one-leg transaction out of scope of the PSD2 RTS on SCA.
- NO Secure Corporate Payment: the Merchant is not capable of highlighting the existing agreement and potential exemption to the ACS/Issuer.
- NO Whitelist Status: the Merchant is not informed if it is whitelisted in the ongoing transaction.

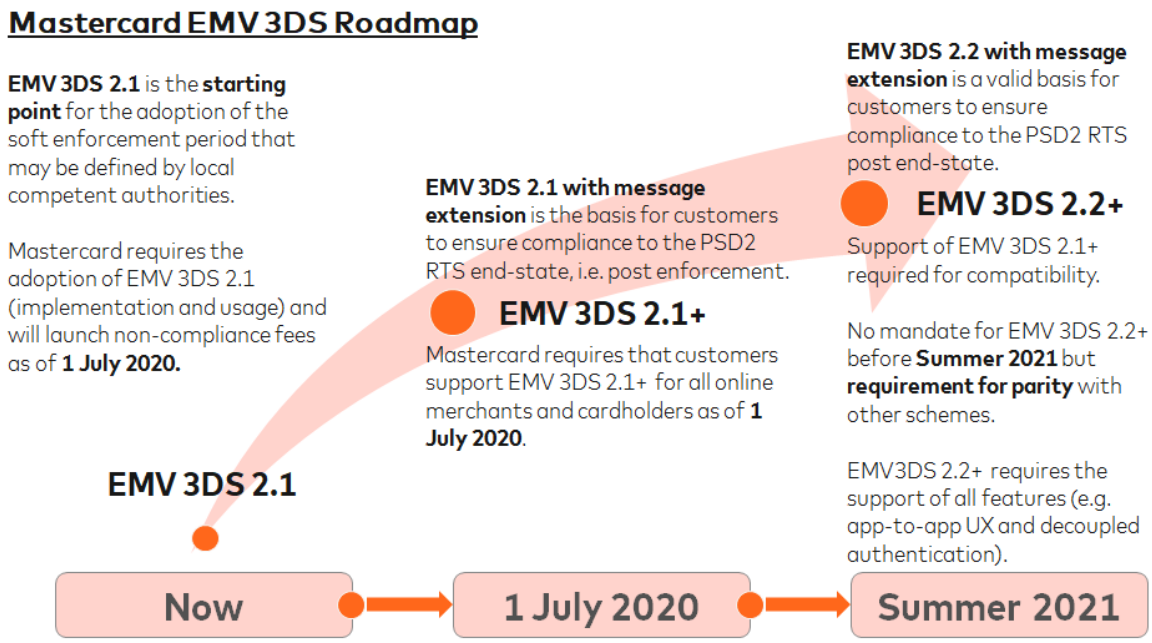
In response to an Acquirer exemption (Field 1="05"), the ACS should respond with an ECI=6 with leading indicators of kN keeping the liability to the Merchant:

- For an EMV 3DS v2.1, an ACS response of Transaction Status = "N" with a new Transaction Status Reason Code of "81".
- For an EMV 3DS v2.2, an ACS response of Transaction Status = "I" with any value in the Transaction Status Reason Code.

The Directory Server rejects the ARes with ECI=6 if the above flagging is not used.

Mastercard EMV 3DS Roadmap

EMV 3DS 2.1 is the basis of the Mastercard Roadmap.



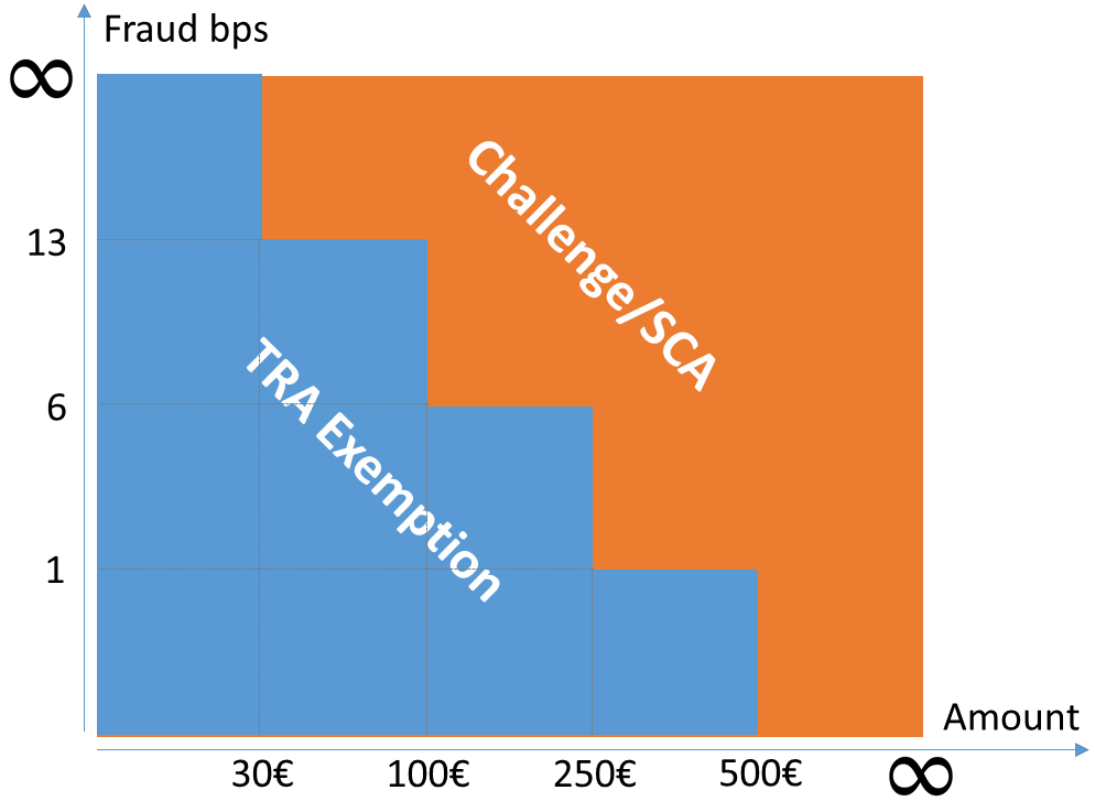
EMV 3DS 2.1+ (EMV 3DS 2.1 + Mastercard PSD2 Message Extension) is the corner stone of the roadmap, allowing Customers to leverage all PSD2 features as from day-one (Acquirer exemptions, whitelisting status, secure corporate payment, SCA delegation). It must be supported by all Customers by mid-2020 (1 July 2020). This leaves six months at a maximum, four and a half months considering the freeze period starting on 15 November 2020, to fine-tune the production setup and end-to-end test the production environment from soft launch to full production by 31 December 2020.

Surfing on that basis, EMV 3DS 2.2 with the Mastercard PSD2 Message Extension (EMV 3DS 2.2+) needs to be supported for all features in the extension that are not supported in the core EMV 3DS 2.2 specifications (acquirer exemptions and whitelisting status). The support of EMV 3DS 2.2+ is not mandated before summer 2021.

Acquirer SCA Exemptions

An Acquirer can apply SCA exemption only if PSD2 RTS conditions are met.

- An Acquirer exemption is available for:
  - **Low-value payments** when the payment is not higher than €30. The Issuer must check if the transaction counter (maximum 5) or cumulative amount (maximum €100) since the last SCA is not exceeded as per PSD2 RTS.
    Refer to the section Low-Value Payments (LVP) and Management of Counters for more information.
  - **Transaction Risk Analysis (TRA)** due to low fraud rate (art 18 – see fraud thresholds for transaction value ranges below). Mastercard plans to monitor compliance by checking if the Acquirer and Merchant fraud rate are below the fraud level in bps.
    * 1 bps = 1 % divided by 100 = 1 out of 10,000



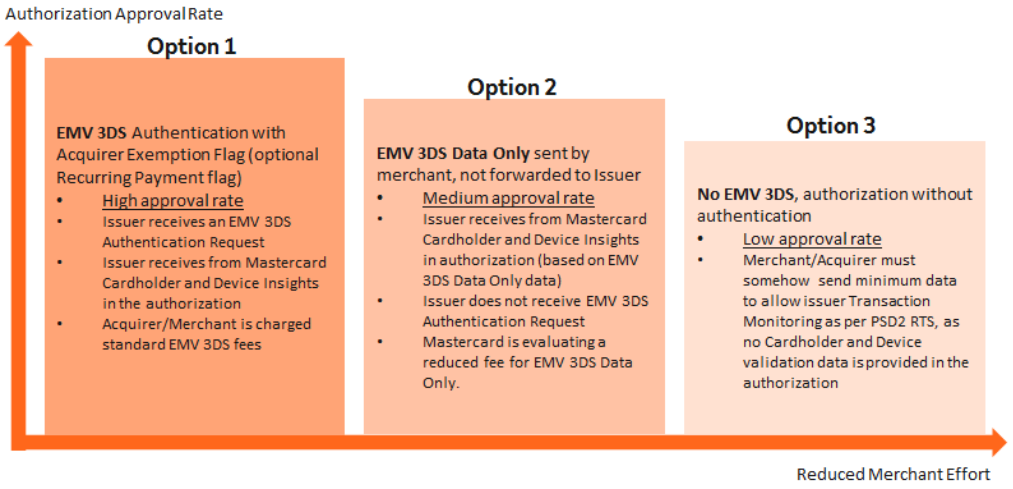
  - **Recurring Payment**[3] if the amount is the same. When the amount varies, the transaction may fall under Merchant Initiated Transactions. Refer to section Merchant-Initiated Transaction (MITs).

[3] Merchant-Initiated Transactions (MITs), when the Cardholder is off-session and the Merchant initiates the payment without any involvement of the Cardholder in triggering the transaction(s) (such transactions are out of scope from PSD2 RTS) are not exempted but excluded, for example out of scope of the PSD2 RTS on SCA.

Decoupled authentications can also be applied (refer to the section Decoupled Authentication).

- The Acquirer/Merchant is liable in case of fraud if the Issuer does not apply SCA.
- Transaction monitoring has to be applied by the Issuer and the Acquirer.

For Recurring Payments and Acquirer TRA exemptions, Mastercard proposes the following three options for Merchants/Acquirers to provide the required information to the Issuer:



The highly recommended option 1 drives the highest authorization approval rate as a full EMV 3DS authentication request with all required data provided to the Issuer for an optimal "decisioning" process.

Option 2 is an intermediate option allowing the Merchant to provide additional data but without going through the authentication process. The Issuer receives cardholder and device insights in the authorization message. The anticipated approval rate of those transactions is lower than fully authenticated transaction (option 1) but higher than no-EMV 3DS (option 3). EMV 3DS Identity Check Insights is flagged with the new SLI 214 being introduced in the third release of Mastercard's core systems. See announcement *AN 2479—Electronic Commerce Security Level Indicators for the Mastercard Identity Check Program*.

It is important to mention that Mastercard will inject valuable risk scoring insights from the additional data provided by the Merchant into the authorization message. These are the Digital Transaction Insights (refer to the section on Digital Transaction Insights). These insights are injected if the additional data is provided by the Merchant in EMV 3DS, even if the Issuer does not support EMV 3DS and only supports 3DS1. The provision of these insights by Merchants allows to train risk models and increase the EMV 3DS footprint to ultimately lead to a trusted EMV 3DS ecosystem. The processing and usage of these insights by the Issuer also improves the authorization approval rates to the benefit of all stakeholders in the authentication value chain.

Mastercard sets minimum quality standards (minimal authorization approval rate and a maximum abandonment rate) whenever EMV 3DS is used.

The Mastercard Identity Check™ Program already requires a minimum authorization approval rate of 90 percent for fully authenticated transactions. As EMV 3DS allows a lot more data to be exchanged, fraud detection should improve vs 3DS 1.0, which is expected to lead to reduced false declines and higher authorization approval rates. EMV 3DS is also expected to reduce authentication abandonments.

Mastercard will monitor on an ongoing basis the Key Performance Indicators (KPIs) of authorization approval rate, authentication abandonment rate and fraud rate. This latter is important to leverage the TRA exemption.

Refer to section Authentication Quality and Key Performance Indicators.

Mastercard's Position for Europe

An authorization in the European Economic Area (EEA) zone (Acquirer and Issuer in an EEA country) without authentication (for example, no EMV 3DS or EMV 3DS Identity Check Insights) is only allowed if an Acquirer exemption or MIT applies as per PSD2 RTS, or if another SCA compliant method is used.

When Strong Customer Authentication by the Issuer is not required under PSD2 RTS, or when it has been delegated, the Acquirer must provide the reason by populating the appropriate value in DE 48—Additional Data—Private Use, subelement 22, subfield 1 in the authorization message.

NOTE: Refer to *Mastercard Rules* for the latest information on this topic. During soft enforcement of the PSD2 SCA regulation, temporary non compliance that this latter regulation is tolerated if a migration plan has been approved by the National Competent Authorities until the applicable grace period ends.

Issuers are recommended to NOT systematically decline authorizations without authentications when these use an Acquirer SCA exemption as per the PSD2 RTS. Additional information provided to the Issuer, through the EMV 3DS Identity Check Insights channel for example, should lead to increased confidence in the transaction to the Issuer. Another option is the use of a soft decline or decline-as-SCA-required (refer to section Soft Decline or Decline-as-SCA-required) by the Issuer when SCA is requested. This will suggest the Merchant to re-submit the request but now with EMV 3DS.

For EMV 3DS Identity Check Insights messages, the AReq uses Message Category = "80". The ARes will return a Transaction Status of "U" (Authentication/Account Verification Could Not Be Performed; Technical or other problem, as indicated in ARes or RReq) with a Transaction Status Reason Code = "80".

The position above has been translated as a requirement for Acquirers to set the Acquirer exemption indicator in the authorization. Also, as a general rule, Issuers are recommended to NOT decline no-3DS transaction without Acquirer exemption or without DE 48—Additional Data—Private Use, subelement 22, subfield 1 for the Issuer should try to apply an Issuer exemption or exclusion (Acquirer outside of EEA, MOTO or MIT) where possible.

Position

NOTE: Refer to *Mastercard Rules* for the latest information on this topic.

In the Authorization Request/0100 message for an intra-EEA Remote Electronic Transaction that is subject to PSD2 RTS, authentication can only be skipped if:

- An acquirer exemption to Strong Cardholder Authentication (SCA) applies
- OR if another SCA-compliant method was used (such as delegation to the merchant, Secure Corporate Payment exemption applied with the merchant's knowledge)
- OR a PSD2 SCA migration plan has been agreed with the National Competent Authorities

When SCA by the issuer is not required under PSD2 RTS, or when it has been delegated, the acquirer must provide the reason by populating the appropriate value in data element (DE) 48, subelement 22, subfield 1 in the authorization message:

01=Merchant Initiated Transaction

02=Acquirer low fraud and Transaction Risk Analysis

03=Recurring payment

04=Low value payment

05=SCA Delegation

06=Secure Corporate Payment

An issuer must be able to process DE 48, sub-element 22, subfield 1 in the authorization message.

Issuers must not systematically decline (including soft declines with RC65) authorizations with DE 48.22.1, even if non-3DS, unless high risk or Low Value Payment exemption counter is exceeded.

Issuers must not systematically step-up authentications with acquirer exemption or delegation flag (in the EMV 3DS version 2.1 Merchant Data Field 1 [SCA Exemptions], value of 05 or 07).

Acquirers in the EEA that allow their online merchants to request a Transaction Risk Analysis (TRA) exemption under PSD2 RTS must set the TRA exemption flag for such merchants when registering them for the Identity Check Program in the Identity Solutions Services Management (ISSM) tool. Mastercard may monitor compliance in the future by verifying if the merchant name used in the authorization message has the right to use the acquirer TRA exemption as specified in the ISSM tool (based on the merchant name registered for authentications).

In order to optimize authorization approval rates for transactions using an Acquirer exemption under PSD2 RTS, it is recommended that Merchants send an EMV 3DS authentication request with Acquirer exemption flag.

EEA acquirers and issuers must ensure that the "acquirer exemption" flag (used for all acquirer exemptions, such as low value payment and TRA exemption and recurring payment) can be supported in EMV 3DS authentication requests.

This must be flagged in EMV 3DS version 2.1 Merchant Data Field 1 (SCA Exemption) with value 05/No SCA Requested, Transaction Risk Analysis performed and effective EMV 3DS v2.2 Challenge Indicator value 05/No SCA Requested, Transaction Risk Analysis performed.

NOTE: When a Merchant is requesting an Acquirer exemption in the authentication, the Acquirer exemption flag also needs to be set in the authorization even if the ACS has accepted the exemption in the authentication (SLI 216).

EEA acquirers with online merchants accepting corporate cards, as well as corporate card issuers, must ensure that the EMV 3DS version 2.1 Merchant Data Field 4 (Secure Corporate Payment) (which indicates if the conditions for the Secure Corporate Payment exemption are met and hence if the exemption can be applied by issuers) can be supported.

Refer to the following document for more information on this topic: *AN 2609—Enhancements to Support the Low-Risk Transaction Indicator for EEA Customers*.

Flagging and Liability Shift Matrix with PSD2

In the table below, SLI217 is optional for European ACS/Issuers in response to an authenticated recurring payment EMV 3DS 2.1 where SLI 212 is recommended.

With EMV 3DS 2.2, SLI217 has to be used by ACS in response to a 3RI authentication request for subsequent payments in a recurring payment arrangement. Acquirers have to support SLI217 on the initial recurring payment authentication request (when setting up the agreement), which gives them fraud chargeback protection.

In the following table:

- Columns 1 and 2 define if Merchants use EMV 3DS or not, and what type of exemption is requested.
- Columns 3 and 4 clarify how those transactions are flagged in authentication and authorization.
- Column 5 specifies the type of action that is expected for those transactions.
- Columns 6 and 7 identify the AAV leading indicators and SLI that appear as a result of those transactions with the expected Issuer action.
- The last column clarifies where the liability stands for those transactions and the expected Issuer action.

In the table, when "3DS Req Chal Ind = 05" is mentioned, this is for EMV 3DS 2.2 as this value does not exist in EMV 3DS 2.1. For this earlier version, the 3DS Req Chall Ind = 02 and the Field 1 of the PSD2 Mastercard message extension = 05.

Merchant	Exemption	Authentication	Authorization	Possible Action	AAV Leading Indicators	SLI	Liability
No 3DS or Identity Check Insights	No exemption			Decline as not compliant		210	Acquirer
No 3DS or Identity Check Insights	LVP		DE 48 SE 22 SF1 = 4	Accept exemption Check LVP counters		210	Acquirer
No 3DS or Identity Check Insights	Acquirer TRA		DE 48 SE 22 SF1 = 2	Accept exemption		210	Acquirer
No 3DS (STA) or Identity Check Insights	RP/MIT first		DE 61 SE 4 = 4 DE 48 SE 22 SF1 not set	Not compliant RC65 to step-up		210	Acquirer
No 3DS (STA) or Identity Check Insights	RP/MIT subsequent		DE 61 SE 4 = 4 DE 48 SE 22 SF1 = 1 or 3	Accept exemption		210	Acquirer
EMV 3DS	No or Any	Based on exemption	Based on exemption	No 3DS	kL or kE	211	Issuer
EMV 3DS	LVP	3DS Req Chal Ind = 05*	DE 48 SE 22 SF1 = 4	Accept exemption Check LVP counters	kN	216	Acquirer
EMV 3DS	Acquirer TRA	3DS Req Chal Ind = 05	DE 48 SE 22 SF1 = 2	Accept exemption	kN	216	Acquirer
EMV 3DS	No or Any except LVP	Based on exemption	Based on exemption	Issuer exemption	kA or kG	212	Issuer
EMV 3DS	No or Any, except RP/MIT first	Based on exemption	Based on exemption	Challenge Reset LVP counters	kB or kH	212	Issuer

Merchant	Exemption	Authentication	Authorization	Possible Action	AAV Leading Indicators	SLI	Liability
EMV 3DS	RP/MIT first	3DS Req Auth Ind = 02 3DS Req Chal Ind = 04	DE 61 SE 4 = 4 DE 48 SE 22 SF1 not set	Challenge	kB or kH kO	212 217 (optional)	Issuer

For DE 48 SE 22 SF 01="01", "02", "03" or "04", the SLI can be 210, 214 or 216 as described in AN 1803—Acquirer Exemptions for Strong Customer Authentication under PSD2 and the RTS. For MITs (value "01"), first transactions uses SLI 212 or 216 (less likely) while subsequent uses SLI 210 or 214. For DE 48 SE 22 SF 01="05" (SCA delegation), only SLI 216 can be used.

Soft Decline or Decline-as-SCA-required

In view of an authorization request without authentication (no- 3DS or EMV 3DS Identity Check Insights), an Issuer may decline the request and indicate at the same time to the Merchant/Acquirer that SCA is required. The Merchant/Acquirer will then initiate a second flow including an authentication request followed by an authorization request.

The Issuer indicates to the Merchant/Acquirer that SCA is required by returning the value 65 (Exceeds withdrawal count limit) in DE 39 of the authorization response. The Merchant receiving a response code of 65 (RC65) will need to go through SCA and will therefore need to flag the:

3DS Requestor Challenge Indicator = "03" (Challenge Requested: 3DS Requestor Preference) or "04" (Challenge Requested: Mandate); "04" for regulated markets.

Until all Issuers and Merchants support RC65, Merchants are recommended to always send an authentication request following an authorization that was declined for non-financial and non- technical reasons (typically authorization response codes 05-"Do Not Honor" and 12-"Invalid Transaction"). It is recommended that the authentication request is sent without asking the consumer to re-enter card details. The Merchant should have a mechanism to re-use card details used for the initial authorization.

As declined authorizations followed by an authentication and another authorization will add an estimated 10 seconds latency, some Cardholders may abandon such transactions.

Merchants are therefore recommended to always send authentication requests, especially with Issuers that decline authorizations without prior authentication.

NOTE: If Merchants go straight to authorization, the authorization has to be done during checkout, for example before goods are actually shipped (clearing has to wait until shipment). Indeed, the Issuer softly declining the authorization will require SCA to occur while the cardholder is still in-session.

It's assumed that the Acquirer in authentication and the Acquirer in authorization are in the same geography (either both outside the EEA or inside). If the authorization Acquirer is in the EEA, a soft decline by the Issuer could result in a transaction not being stepped up/challenged if the authentication Acquirer is outside the EEA.

Acquirers are requested not to normalize the error codes to their merchants so that these are aware of RC65.

The Acquirer exemption with authentication is indicated by SLI 216.

In this case, the AAV is provided. A new AAV prefix should be used by Issuers in this case to avoid Merchants using the AAV to flag the authorization as fully authenticated and benefit from liability shift.

In this case, the Acquirer is liable in case of fraud, except if the Issuer decides to step up. If the Issuer decides to step up, the SLI used is 212, for example both the Merchant and the Issuer are UCAF-enabled.

RC65 should not be used by Issuers and Mastercard will closely monitor Issuer behavior in the case where:

- the transaction is fully authenticated (SLI 212) above 30€ or equivalent in other currencies
- the transaction is SCA exempted (SLI 216 and SLI 217)

PSD2 SCA Exemptions and Maestro

Currently there are three special programs enabling ecommerce European Merchants to accept Maestro transactions without 3DS (see *Transaction Processing Rules* Europe Region 5.3).

The programs are:

- Maestro Low Merchant Risk Program (MLRMP)
- Maestro Utility Payment Program (MUPP)
- Maestro Recurring Payment Program (MRPP)

MLRMP, MUPP and MRPP participating Merchants are subject to eligibility and operations requirements that are specified in the *Europe Operations Bulletin December 2011* and *Europe Region Operations Bulletin March 2016*.

Currently MLRMP, MUPP and MRPP participating Merchants use specific values:

- SLI 213
- Mastercard-assigned Merchant ID
- Static AAV

These specific values are peculiar to these special Maestro programs and they are not used for Mastercard.

From the PSD2 RTS on SCA effective date:

- Ecommerce European Merchants who want to accept Maestro transactions without Strong Customer Authentication will be able to do so only if an RTS regulated exemption applies;
- The above Maestro specific values will come to an end (SLI 213, Mastercard-assigned Merchant ID, static AAV);
- Merchants who want to leverage Acquirer exemptions have to follow the same use cases and specifications for Mastercard and for Maestro.

Low-Value Payments (LVP) and Management of Counters

As per the PSD2 RTS, payments are considered as low value if less than or equal to 30 euros or equivalent in other currencies.

The most recent update on the EBA position on necessary currency conversion can be found at:

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4040

The PSD2 RTS also set maxima above which SCA will be required:

- Maximum number of consecutive transactions without SCA = 5
- Maximum cumulative amount of transactions without SCA = 100 euros or equivalent in other currencies. Mastercard recommends the management of LVP counters based on the amount to reduce the number of challenges.

The LVP exemption can be applied by Issuers but as well by Acquirers.

Because Acquirers are not able to count the number of transactions and cumulative amount since the last SCA, this must be done by the Issuer authorization host system during authorization processing especially when Acquirers apply the LVP SCA exemption without sending an authentication request. When these counters or cumulative amount limits are exceeded, Issuers should respond with response code 65 and Merchants should send an authentication request (refer to section on Soft Decline or Decline-as-SCA-required).

A LVP exemption will be indicated by the Merchant/Acquirer by 3DS Requestor Challenge Indicator = "05" in authentication and DE48 SE22 SF1 = "04" in authorization.

The management of counters by Issuers should only be done in case of Acquirer exemption flagged as LVP in the authorization, and not in the case of Acquirer exemption flagged as TRA in the authorization message. An Acquirer TRA exemption for a purchase amount less than or equal to 30€ should not trigger the management of counters.

NOTE: In authentication, an ACS does not know if a value of "05" in the 3DS Requestor Challenge Indicator indicates a LVP exemption subject to counters management or TRA exemption not subject to counters management. In this case, the ACS should not apply the LVP counters in authentication processing if the amount is less than or equal to 30€, assuming the TRA exemption applies. This is combined with the checking of the LVP counters in authorization if the LVP exemption is flagged in authorization. If SCA is needed, a RC65 should be issued by the Issuer host based on which Acquirers should retry with EMV 3DS without Acquirer exemption.

When the counter threshold has been reached, requiring the transaction to be stepped up, the Issuer should not soft-decline the transaction if a TRA exemption can be applied, for example, if all conditions to apply this exemption are met. This will avoid unnecessary step-ups and potential abandonment.

Arguments for the adoption of a TRA exemption by the Issuer are:

1. This only applies to low risk transactions as Acquirers must have performed Transaction Monitoring when they apply LVP exemption (which includes checking signs of malware infection, checking if compromised authentication elements were used).
2. When Issuers apply TRA, they have to perform incremental checks on top of Transaction Monitoring (for example, checking signs of malware infection and checking if compromised authentication elements were used is not needed anymore, given that this was already checked by the merchant/Acquirer when they applied low value payment exemption). Issuers only have to check on top of Transaction Monitoring transaction history, fraud patterns, card holder and merchant location, logs, all of which can be done using authorization data (hence EMV 3DS data is not needed).

In this case of TRA exemption applied by the Issuer, the liability for the transaction remains with the Merchant because:

- the Merchant requested a LVP exemption straight in authorization, without going through the authentication flow before
- the Merchant decided to take the liability at the time of requesting a LVP exemption in authorization
- the application of an Issuer TRA exemption is not recognizable in the authorization message

The LVP Issuer exemptions should therefore be handled as follows:

1. The Merchant sends a regular EMV 3DS authentication request (for example, does not apply an exemption, which is probably unusual as most Merchants will want to apply the LVP exemption themselves);
2. The Issuer applies its LVP exemption and responds with a frictionless approval in the authentication response (for example, with ECI=2);
3. The Acquirer sends a fully authenticated authorization with AAV (with leading indicator "kA" for frictionless);
4. The Issuer authorization processor, based on the AAV with leading indicator "kA", checks:
   a. Can the issuer apply other exemptions than LVP (TRA or whitelisting)? If so, then the Issuer bypasses LVP counters;

b. If the Issuer LVP exemption must be applied (no other issuer exemption available) then check LVP counters.

5. If the Acquirer receives a soft decline (RC65) then the Merchant must send another EMV 3DS authentication request with challenge indicator.

Merchant Whitelisting

Refer to the following document for more information on this topic: *Mastercard Standards for Merchant Whitelisting v1.0*.

Secure Corporate Payments

The PSD2 RTS Article 17 states that Secure Corporate Payments or Business-to-Business (B2B) Payments over dedicated payment processes and protocols are exempt and that this exemption applies to "payment processes or protocols that are only made available to payers who are not consumers, where national competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security" to those achievable with SCA.

The Secure Corporate Payment is an Issuer exemption, meaning that it can only be invoked by the Issuer. The merchant should send an authentication request, unless the merchant has a way of recognizing the transaction as secure corporate payment exempted, in which case the merchant can send the transaction directly for Authorization.

For exempt transactions, the Issuer is not required to challenge the account holder and carry out two-factor authentication. Instead, the Issuer can respond to authentication requests with a risk-based authentication (also known as "passive" or "silent" authentication in the Travel industry) or alternatively approve transactions that are sent straight to authorization.

Although the decision is with the competent authority of each Member State, Mastercard's position is that lodged and virtual corporate/commercial cards should be exempt from SCA:

- **Lodged cards**: A commercial card that is lodged with a company-approved third party, such as a travel company that books travel and hotels on behalf of the company by a secure, dedicated payment process and protocol. Use cases include both traditional company travel procurement (via a company-approved travel agency) and broader business-to-business procurement, where commercial cards are lodged both securely and directly with approved company suppliers. Lodged cards may include physical/plastic cards issued to individual employees for business expenses and with corporate liability.
- **Virtual Card Numbers**: Virtual card numbers (VCNs) are used over dedicated payment processes and protocols, and ensure a very high level of security. The generation of VCNs is protected with SCA and the VCN can be uniquely linked to the applicable Merchant or other parameters that further control its use (such as, transaction value, validity period, and currency).

For corporate payment transactions, two scenarios are possible:

1. **Centrally billed Lodge and Virtual Cards where the product as a whole is exempt.**
   The Secure Corporate Payment exemption is critical for centrally billed lodge and virtual cards as there is typically no cardholder associated with the product and available to perform a step-up authentication.

   Options:

   – Risk-based authentication: For exempt products, Issuers should respond to authentication requests with a risk-based authentication.
     The products can be identified by the Issuers & their ACS based on the product/PAN and Issuers can indicate to merchants (via their ACS) that SCA is not required. It is recommended that Issuers inform their ACS of card numbers or card ranges that can use this secure corporate payment SCA exemption (such as, the card number is a lodged account or virtual corporate card number) to avoid step-up. ACS services needs to apply a risk-based authentication for these transactions to comply with Transaction Monitoring under PSD2 RTS.
   – No Authentication: Mastercard guidelines allows for authentication to be skipped and for transactions to be sent straight to authorization if an Acquirer exemption to SCA applies, if another SCA compliant method was used such as the Secure Corporate Payment exemption applied with the merchant's knowledge, OR if a PSD2 SCA migration plan has been agreed with the National Competent Authorities. This option should only be used where the merchant is certain that an exemption applies. In case the issuer deems that the transaction is not subject to a secure corporate payment exemption, the issuer should respond the authorization request with a soft decline. Soft declines may ultimately result in a hard decline, especially in travel where there are often several parties involved in the authentication meaning soft declines can be difficult to execute.

2. **Physical/ plastic Corporate Cards issued to employees where typically only certain transactions are exempt**
   When used at physical or online POS without dedicated processes or protocols, such as for ecommerce transactions on a public website, SCA needs to be applied.

   When cards are lodged with trusted suppliers using Secure Corporate Payment processes and protocols (such as, online bookings via corporate travel agents) transactions may be considered exempt under Article 17.

   As a result, for physical/plastic Corporate Cards Issuers need the acquirer to provide an indicator/flag for the Issuer to be able to recognize that the specific transaction originating from a Secure Corporate Payment process and protocol. The Issuer is not able to determine this solely based on the card number/ PAN.

   Options:

   – Step-up/ two-factor authentication with the Cardholder
   – Risk-based authentication:
     – To enable the merchant to indicate to the issuer in the authentication that a Secure Corporate channel was used, Mastercard has included a Secure Corporate Payment flag in Field 4 of the EMV 3DS 2.1 and EMV 3DS 2.2 –PSD2 Message Extension

  - Where the 3DS Server populates this flag in the authentication message with YES to indicate a Secure Corporate Payment channel such as the GDS channel, the issuer ACS can use the flag in combination with the Corporate Card PAN to apply a risk-based authentication and improve the user experience.
- No authentication: Mastercard guidelines allow for authentication to be skipped and for transactions to be sent straight to authorization if an Acquirer exemption to SCA applies, if another SCA Authentication compliant method was used such as Secure Corporate Payment exemption applied with the Merchant's knowledge, OR if a PSD2 SCA migration plan has been agreed with the National Competent Authorities. In case the issuer deems that the transaction is not subject to a secure corporate payment exemption, the issuer should respond the authorization request with a soft decline. Soft declines may ultimately result in a hard decline, especially in travel where there are often several parties involved in the authentication meaning soft declines can be difficult to execute.
  The flag '06' to indicate Secure Corporate Payment is available in data element (DE) 48, subelement 22, subfield 1 in authorization.

NOTE: Where merchants request authentication from the Issuer, liability shifts to the Issuer. Conversely, if merchants send transactions directly to authorization, liability remains with the merchant.

Secure Corporate Payment Flags

Mastercard has implemented flags in both authentication and authorization to allow the merchant/acquirer to indicate that a secure corporate payment channel was used. These flags are critical for physical plastic cards since for these products the issuer cannot identify a Secure Corporate Payment transaction solely based on the card number/PAN.

Flag in Authentication

The Mastercard PSD2 Message Extension to the current EMV 3DS 2.1 and EMV3DS 2.2 specifications

- Field 4 in AReq: Transaction used dedicated processes or protocols as per RTS article 17 (Secure Corporate Payment Exemption for Issuer)
- Flag set to YES to indicate Secure Corporate Payment (default is NO)

Field #	Field	Field Definition
4	Secure Corporate Payment	Whether the electronic payment transaction uses dedicated payment processes or protocols under PSD2 RTS Article 17's Secure Corporate Payment Exemption, which the Issuer can apply

Flag in Authorization

DE 48, subelement 22, subfield 1 to indicate that Secure Corporate Payment processes and protocols have been used for the transaction (Article 17).

Value '06' = Secure Corporate Payment

Value '06' is effective 5 November 2019.

Recommendations

In order to ensure successful transactions, Merchants should not drop a transaction if issuer does not support 3DS. This is an existing Mastercard rule, which was re-emphasized in digital security roadmap announcements in Q1 2018.

However, as instances have been reported where merchants may have dropped transactions where the Issuer does not support 3DS, Issuers are recommended to enroll all products, including VCNs and Lodged cards in Identity Check and with an ACS provider.

This allows the issuer to respond with a risk-based authentication for transactions exempt from SCA under Secure Corporate Payment (Art 17) based on the applicable BINs, BIN ranges or PANs.

Issuers should ensure their processor can manage the Secure Corporate Payments exemption and ensure that they do not systemically decline authorization requests without 3DS where the Secure Corporate Payment exemption applies.

Out of the Scope of the PSD2 RTS

The following are out of the scope of the PSD2 RTS.

Anonymous Prepaid Cards

Due to their very nature, payments made through the use of an anonymous payment instruments, such as anonymous prepaid (such as, gift) cards, are not subject to the obligation of strong customer authentication.

The Issuer is the only one able to identify this type of cards. The Acquirer will not be able to identify from the primary account number that the product is an anonymous product.

There is indeed no specific Mastercard product code or Mastercard BIN associated to the anonymous nature of the payment instrument.

However, an account range indicator ("Anonymous indicator") was introduced in October 2019 (4th Release of Mastercard's core systems). The Anonymous Indicator signals to Acquirers whether a Mastercard and Maestro prepaid account range is anonymous or non-anonymous.

Refer to the following document for more information on this topic: *AN 2509—Announcing the Prepaid Anonymous Indicator ("Anonymous Indicator")*.

NOTE: There may be prepaid programs requiring Customer due diligence where the name of the Cardholder (what the Merchant sees) is not mentioned but that are non-anonymous cards in the PSD2. This is the case of some instantly issued types of cards.

Mastercard Rules allow Issuers not to register Anonymous Prepaid Cards on the Identity Check Authentication Network. If there is concern that Merchants refuse cards when the Authentication Request would result in an Attempt due to expectation of lower approval rates then Issuers may need to consider registering these cards anyway.

Mail Order/Telephone Order (MOTO)

The PSD2 RTS is not covering Mail Order/Telephone Order (MOTO) transactions.

In authorization messages, MOTO transactions are flagged by a value of 2 (Cardholder not present - mail/facsimile order) or 3 (Cardholder not present - phone or Automated Response Unit [ARU]) in DE 61 SF 4.

When purchases have been ordered by mail or telephone, flagging MOTO transactions in the correct way is the responsibility of the Merchant and the PSP/Acquirer. To avoid confusion in the CNP environment about the method used to order the purchase, Merchants have to properly code MOTO transactions to ensure that Issuers can make appropriate SCA decisions.

In EMV 3DS 2.2, specifications, the value 08 (Mail Order) or 09 (Telephone Order) in the 3RI Indicator will indicate a MOTO transaction.

Voice commerce (aka. vCommerce) transactions, leveraging user interaction with voice recognition technology, will generally require SCA (unless an exemption applies).

One-leg Transactions (one leg in the EEA, the other out)

The PSD2 RTS generically refers to Payment Service Providers (PSPs) to identify parties that are either managing the acceptance and/or the issuance of electronic remote card-based payment transactions.

Mastercard is translating this into Acquirer and/or Issuer since these are the legal entities that are Customers of Mastercard.

The locations of the Issuer and Acquirer are relevant to determine if the RTS SCA requirements apply to two-leg transactions. Thus, it is sufficient that the Issuer and the Acquirer are located in the EEA for the RTS to apply.

The location of the cardholder and Merchant is in principle not relevant. However, the Acquirer country code may not be known by the Issuer (if no authentication or if the authentication does not provide the Acquirer country code in the PSD2 Mastercard message extension). Mastercard has asked the EBA to confirm that the Issuer is allowed to use the Merchant's location as a proxy/fallback (in lieu of the Acquirer's location) to determine whether the Acquirer is located in the EEA.

Under PSD2, a card in the EEA must be issued by an Issuer in the EEA. If the card is issued in the EEA, the Issuer is also in the EEA and is subject to the PSD2 SCA requirements.

On the acquiring side, the Acquirer must be licensed in the EEA[4] to acquire Merchants in the EEA. If the card is issued in the EEA and the Merchant is in the EEA, the Issuer and Acquirer are in the EEA and transactions are "two-leg" transactions. This also means that when the Merchant is in the EEA, the Acquirer country code in the PSD2 Mastercard message extension should not be taken into account by the Issuer to determine if the transaction is two-leg in scope of the PSD2 RTS (our proxy position). It will be by default.

If the Issuer is in the EEA and the Merchant is not in the EEA but is acquired by an Acquirer in the EEA, the Merchant country code would give the impression to the Merchant that the transaction is "one-leg" not subject to the PSD2 SCA requirements. As the PSP/Acquirer is in the EEA, PSD2 SCA requirements apply.

Mastercard's Position for Europe

If the issuer and the acquirer are in the EEA but the merchant is not, EMV 3DS authentication requests must include the EMV 3DS version 2.1 Merchant Data with Field 3 (acquirer country code) containing the acquirer country code. In other cases, Mastercard recommends to provide the acquirer country in the EMV 3DS version 2.1 Merchant Data Field 3.

NOTE: Refer to *Mastercard Rules* for the latest information on this topic. During soft enforcement of the PSD2 SCA regulation, temporary non compliance that this latter regulation is tolerated if a migration plan has been approved by the National Competent Authorities until the applicable grace period ends.

The issuer and its Access Control Server are recommended to use the acquirer country code in the EMV 3DS version 2.1 Merchant Data Field 3 to determine if SCA is required by PSD2 RTS. If the acquirer country code is not provided, then issuers are recommended to use the merchant country to determine if SCA is required by PSD2 RTS.

[4] Mastercard understands that certain non-EEA airlines are acquired by an EEA Acquirer. If a non-EEA airline uses an EEA Acquirer, EEA Issuers may decline a no-3DS authorization without Acquirer exemption. To avoid this, these non-EEA airlines are recommended to use 3DS or to flag the authorization with an Acquirer exemption flag if that can be applied. Airlines Merchants are recommended to use the correct Merchant country code.

How to Recognize Acquirer/Issuer Country to Apply SCA Under PSD2

In order to properly identify transactions that are "two-leg" subject to the PSD2 SCA requirements, the EMV 3DS specifications have been amended to include the Acquirer country code (refer to section, EMV 3DS Support of the PSD2 RTS on SCA).

EMV 3DS 2.1 and EMV 3DS 2.2—Mastercard Message Extension

Field #	Field		Field Definition
3	Acquirer Code	Country	Acquirer country code is required when the Acquirer country differs from the Merchant country and the Acquirer is in the EEA (such as, an Acquirer in the EEA acquiring an airline Merchant in the US). If both Acquirer and Issuer are in the EEA, PSD2 SCA requirements apply

The following elements apply as well in the identification of the Acquirer and Issuer countries:

- The Issuer country is identified by the BIN related to the PAN being used. The Member Parameter Extract (MPE) table allows to associate the Issuer country related to a BIN.
- Similarly, the Acquirer country is identified by the Mastercard Customer ID hosted in the DE32 of the authorization message. The Member Parameter Extract (MPE) table IP0072T1 (Expanded Member ID Master) maps the Mastercard Customer ID to the Acquirer country.
- Merchants may not have received from their Acquirer(s) an extract of the MPE tables. If this is the case, Merchants can obtain the BIN table, called the BIN Table Resource, from Mastercard.

The BIN Table Resource provides a list of active and valid issuing account ranges to help Merchants and service providers successfully accept Mastercard transactions and prevent valid accounts from being declined.

Value-add to Merchants:

Reliability	Accurate lists are provided directly by Mastercard—the most reliable source for up-to-date information
Efficiency	With direct access to information, there is no need to continually monitor unauthorized lists
Insight	Helps improve routing, fraud "decisioning", information on brand, product and authorization.

The BIN Table Resource provides authorization parameters ensuring greater BIN information accuracy:

- **Acceptance Brand:** Identifies whether an account range is used for issuing credit, debit, or private label cards;

- **Authorization Only:** Identifies accounts from which a private label or prepaid card has been issued to provide Cardholder with prefunded discount or prepaid value only redeemed at select Merchants at checkout;
- **Issuing Country Code:** Assists in e-commerce fraud management to help detect inconsistencies between the IP address of the originating purchase and the Cardholder billing address that may warrant additional analysis.
- **Local Use:** Identifies whether cards within the authorization account range may be used outside of the country of issuance;
- **Brand Product Code:** Identifies the Mastercard accepted brands: Mastercard Credit, Mastercard Debit, Maestro, Cirrus, Mastercard Private Label;
- **Series 2 BINs:** Range of BINs that begin with "2" and are processed the same as the series "5" BINS.

Merchant-Initiated Transaction (MIT)

Merchant-Initiated Transactions are payments initiated by the Merchant without the interaction of the payer. They are characterized by a lack of involvement of the payer in triggering each individual payment.

Such payments require that:

(1) SCA is applied to the first transaction/action mandating the Merchant to initiate payment(s) and (2) there is an agreement between the payer and the Merchant for the provision of products or services and potential costs associated with these. Such payments can happen in the following cases:

- Recurring Payments for fixed or variable amounts.
- Merchant funded installments.
- The final amount is higher than the amount used at authentication time. This can happen when additional charges are added to the initially agreed amount.
  Such as, a minibar in a hotel or fines with a rented car. The Merchant should anticipate as much as possible these potential additional charges but in some cases, the predefined amount may be reached, thus leading to re-authentication for the incremental charge.

Recurring payments may be initiated at a POS terminal with a PIN (CHIP&PIN) or by contract signature as authentication. This is a use case where operators start a recurring payment agreement with the consumer in store based on consumer authentication (and likely an authorization ASI to validate the PAN) and then send in batch mode a file to their Acquirer to submit subsequent recurring payments.

Merchants bear liability for MITs. However, the liability shifts to the Issuer if:

- 3DS is used and serves Issuer transaction monitoring purposes (see below)
- 3RI is used in EMV 3DS 2.2 for subsequent recurring payments (SLI 217)

Acquirers subject to PSD2 RTS are only allowed to apply Merchant Initiated Transactions (MIT) when:

- The transaction is triggered by the merchant and the cardholder is typically off-session (off-session means the cardholder is no longer interacting with the merchant page or the merchant app), or
- The transaction is triggered by the merchant as it could not have been triggered by the cardholder during checkout, because:
  - The final amount is not known during the checkout (for example, online groceries shopping), or
  - An event triggered the transaction after the checkout (for example, miscellaneous rental or service charges), or
  - The transaction is part of a recurring payment arrangement, or
  - The transaction is broken down into different payments happening at different times (for example, installments, travel bookings, market places), or
  - The transaction is a staged-wallet funding transaction.
    , or:
  - The transaction follows a declined authorization at a transit validator but the customer has completed a billable journey (Transit Debt Recovery).

To set-up each individual MIT, SCA is required, as well as an agreement between the merchant and the cardholder specifying the reason for the payment and the payment amount (or an estimate when the precise amount is not known).

The MIT exclusion cannot be used to bypass the PSD2 SCA requirements for transactions for which card data has been registered on file with the merchant and the cardholder triggers the payment (Card-on-File).

The EMV 3DS specifications are supporting MITs as follows:

EMV 3DS 2.1	3DS Requestor Challenge Indicator = "02", AND PSD2 Mastercard Message Extension Field1 "Acquirer SCA exemption" = "05" / No challenge requested (transactional risk analysis is already performed)
EMV 3DS 2.2	3DS Requestor Challenge Indicator = "05" / No challenge requested (transactional risk analysis is already performed)

Mastercard recommends that Merchants send EMV 3DS (with 3DS Requestor Challenge Indicator = "02" so that Issuers are instructed not to step-up) as it provides the data to the Issuer to check, for example, if device authenticators are compromised (which is required under Transaction Monitoring).

Issuers are required to NOT systematically decline MIT with no-3DS authorization and not step-up if EMV 3DS is used. As MIT is not part of PSD2 RTS and given the importance of MIT, Mastercard monitors Issuer behavior when handling MIT.

Mastercard's Position for Europe

MIT must be flagged by populating DE 48, subelement 22, subfield 1 in the authorization message with 01 = Merchant Initiated Transaction. Refer to release announcement *AN 2609—Enhancements to Low- Risk Transaction Indicator to Support EEA Customers Compliance to PSD2 RTS* for more details.

NOTE: Refer to *Mastercard Rules* for the latest information on this topic. During soft enforcement of the PSD2 SCA regulation, temporary non compliance that this latter regulation is tolerated if a migration plan has been approved by the National Competent Authorities until the applicable grace period ends.

When setting-up an MIT includes an authorization request, its Trace ID must be provided by the EEA acquirer in subsequent related authorizations in DE 48, subelement 63 (Trace ID). Refer to release announcement *AN 2630—Use of Trace ID to Support PSD2 Recurring Payment Requirements* for more details.

The Trace ID should not be included in the initial authorization at setup of the MIT, and should only be included in subsequent authorizations. Issuers should not decline authorizations because of the presence of non-relevant data elements in messages (such as, presence of a Trace ID in an initial MIT).

If the initial authorization occurred before 14 September 2019, and the initial Trace ID is not available (for example, was not stored), or if the recurring payment was set-up via mail order, telephone order, or via face to face and the initial Trace ID is not available, then the Trace ID must have the following values:

Positions 1–3 = value "MCC" for Mastercard Card

Positions 4–9 = value "999999"

Positions 10–13 = value "1231"

Positions 14–15 = blank filled

Transit debt recovery transactions may also use the dummy trace ID values when the original trace ID information is not present and unable to match.

EEA issuers must be able to process the Trace ID provided in authorizations in DE 48 subelement 63 (Trace ID), for example to validate if an initial SCA occurred to set-up the MIT as required under PSD2 RTS.

To ensure compliance with the PSD2 RTS, Issuers need to check if SCA applied to initial recurring payments or MITs. The storage of the initial authorization with SCA is therefore required until the recurring payment or MIT arrangement is cancelled.

The rule to reference the initial Authorization's Trace ID does not apply to reversals, which must continue to include the Trace ID of the authorization to be reversed. More details about how to handle recurring payments can be found in Chapter 5, Card-Not-Present Transactions, Europe Region, 5.4 Recurring Payment Transactions of the *Transaction Processing Rules*.

In cases where a recurring payment is not setup electronically (such as, via MOTO) or is setup in a non-remote (face-to-face) environment (CHIP&PIN at POS or signature), the Trace ID is set

to the above-mentioned dummy value. This is because the Issuer does not need to check for recurring authorizations that an initial SCA happened in these cases (out of scope of SCA requirements).

Usage of Account Status Inquiry (ASI)

To comply with PSD2 and SCA, most remote electronic payments must have been authenticated, typically using an initial 3DS authentication (or using an alternative SCA compliant method).

To inform the issuer that SCA took place, the first authorization (for example, a recurring payment or merchant initiated transaction) must therefore be flagged as 3DS with a valid AAV in DE 48, subelement 43.

NOTE: If the authentication data is passed in an account status inquiry (ASI) and the first actual payment therefore does not contain Service Level Indicator 211 or 212, then the authentication cannot be used to provide the merchant with chargeback liability protection. The chargeback rules require the authentication data to be in the first financial transaction.

Manual Card Entry

Transactions may be presented to Issuers after Manual Card Entry also known as PAN Key Entry (PKE).

This type of transactions is already processed by Issuers now. In the PSD2 context, the following applies for manually card entered transactions under the following conditions:

Conditions	SCA conditions and Issuer behavior
Cardholder is present and card is present	SCA is required. This may require an infrastructure upgrade to support CHIP and PIN in some industries (such as, hotels).
Cardholder is present and card is not present	May be out of scope and should not be systematically declined by Issuers (for example, because it is not an electronic nor a remote transaction, or because it is a MIT).
Cardholder is not present and card is not present	May be out of scope and should not be systematically declined by Issuers (for example, because it is a MIT, or because it is resulting from a booking over the phone).
Recurring Payment where the initial transaction has been strongly authenticated (for example. online reservation)	Subsequent PKE transactions qualify as MIT. There is a need for reconciliation between the initial and subsequent transactions and a reconciliation infrastructure has to be available (such as, hotel properties).

Conditions	SCA conditions and Issuer behavior
Recurring Payment where the initial transaction was a MOTO	Subsequent PKE transactions qualify as MOTO.

Special Purpose Institutions

Under PSD2, Member States may exclude certain 'special purpose institutions' from the application of all or part of the provisions of PSD2 (Article 2(5) PSD2).

As an example, the UK has exercised this option under the UK Payment Services Regulations of 2017 implementing PSD2. These UK Regulations do not apply expressly to (1) credit unions, (2) municipal banks, and (3) the National Savings Bank.

Other countries have also exercised this option: Austria, Belgium, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Poland, Portugal, Slovenia, Spain, and Sweden.

Chapter 4 Specific Use Cases under PSD2

This section contains information on specific use cases for in-session and off-session payments.

General Flow for All Use Cases

The following general flow is applicable to all use cases that are listed under "Use Cases for In-session Payments" and "Use Cases for Off-session Payments". The specifics of each of these use cases are provided in the related section.

- The Merchant sends an EMV 3DS authentication request for an amount that is called the authentication amount. The amount to be indicated depends on the use case that is described in the following sections.
  - In case of Recurring Payment, the 3DS Requestor Prior Transaction Reference captures the DS Transaction ID of the initial Recurring Payment Agreement authentication. This reference is required to complete the authentication process successfully.
  - In case of an MIT, the 3DS Requestor Prior Transaction Reference captures the DS Transaction ID of the initial MIT Agreement authentication. This reference is required to complete the authentication process successfully and must be provided in subsequent authentications where the Merchant is looking for an Issuer authentication when consumer is out-of-session.
- The ACS decides to go for a challenge or risk-based authentication (RBA requiring Issuer exemption) and generates an authentication code (AAV).
  - The Cardholder needs to be in-session in case of challenge.
  - If not, subsequent Merchant-Initiated Transactions may be leveraged or a decoupled authentication may be applied (refer to section Decoupled Authentication).
- The Acquirer presents the authorization (possibly delayed) including:
  - The AAV
  - In case of Recurring Payment or MIT, DE 48 SE 63 captures the Trace ID of the initial Recurring Payment Agreement or MIT
  - The DS Transaction ID
- In the case where EMV 3DS is used, Mastercard injects Digital Transaction Insights (refer to section Digital Transaction Insights) into the authorization request to provide the Issuer with an assessment of the EMV 3DS provided data.
- The Issuer authorizes the transaction upon:
  - Retrieving the original authentication using the 3DS Transaction ID
  - Validating the original AAV (see remark above for Recurring Payments)
  - Dynamic Linking of authentication vs. authorization by
    - (For non-Recurring Payments) Comparing the authorization transaction amount (possibly accumulated) to be less than or equal to the authentication amount. If not possible (such as the amount has changed), the AAVs in authentication and authorization are compared.

Amounts to be Used

The following table presents various use cases and the amount to be used. The use case descriptions and specifics are provided in the following sections.

Use Case (refer to sections below)	Authentication (aka AuthE) Amount
Plain vanilla e-commerce	AuthE Amount = Purchase amount
Delayed delivery/charge/free trial	AuthE Amount = Purchase amount
Partial/split shipment	AuthE Amount = Purchase amount + capped partial shipment costs
Agent Model	AuthE Amount = Total amount
Unknown/undefined final amount before Purchase	AuthE Amount = Pre-agreed purchase amount plus the typical margin in business
Recurring payment with fixed amounts	AuthE Amount = Subscription amount [5]
Recurring payment with variable amounts	AuthE Amount = Maximum expected amount of the Recurring Payment Agreement [5]
Recurring payment combined with one time purchase	AuthE Amount = Purchase amount + subscription amount
Installments	AuthE Amount = Total of all installments including fees and interest

A zero amount reduces the abandonment risk but increases the chargeback risk because the cardholder could claim that the transaction amount was not authorized. An estimate of the final amount may increase the abandonment rate but decrease the chargeback rate. Customers reasonably expect the first payment amount to be authenticated.

Use Cases for In-Session Payments

In-Session Payments are conducted when the Cardholder is available behind his device to perform SCA.

This includes:

- Regular ecommerce transactions
- Delayed Delivery / Charge
- Partial/Split Shipment
- Agent Model

[5] In case of recurring MITs, an authentication for a zero amount may be used. The Merchant will still need to inform the cardholder about the expected amount in agreement.

- Unknown Amount before purchase

Delayed Delivery/Charge/Free Trial

This is a use case when for example there is a trial of a product and payment is made after the trial period, or could be a pre-order of a product with payment before delivery.

Global recommendation: Mastercard highly recommends that transaction is authenticated while the Cardholder is in-session and sent to authorization or pre-authorization. Clearing is delayed till the time of delivery of product. This ensures a smoother process without requiring multiple authorizations or pre-authorizations or holding AAVs for extended periods. If the delay is longer than 7 days or 30 days, respectively applicable for Maestro and Mastercard, then the pre-authorization needs to be extended for another month. This latter process can be repeated if and when needed. As from the second pre-authorization, the AAV is not included but the Trace ID of the initial pre-authorization needs to be provided.

NOTE: The trace ID for recurring payments and MITs needs to be used with the Acquirer Exemption Indicator in DE 48 SE 22 SF 1. If this latter is present, the authorization cannot be an incremental authorization or extended pre-authorization.

There is still the option of sending the authorization after the trial period is over (an Account Status Inquiry[6] or ASI in authorization following the authentication may be envisaged). The transaction is fully authenticated, with chargeback protection in case of fraud. A Merchant needs to refresh the AAV when the retention period has been exceeded and the transaction has not been authorized nor cleared yet.

Partial/Split Shipment

This is a use case when, for example, ordered products are not all available at the same time and the Merchant decides to ship them separately.

Global recommendation: Mastercard highly recommends that the transaction is authenticated for the full amount (purchase amount + capped partial shipment costs) while the Cardholder is in-session and sent to authorization for the full amount.

Multiple clearing transactions are sent based on each of the shipments with the proper partial/final presentment message reason codes. This is in line with the best practices in the Mastercard CIS manual.

When Merchants are from various geographies and only part of the basket is in regulation (such as, part of the split transaction is within the EEA), then the PSD2 RTS on SCA applies unless an exemption can be leveraged.

Agent Model

Agent Model is a use case when for example, an agent manages orders of both hotel and airline from different Merchants. The authenticator is the agent but payments are managed by

[6] An AAV should not be included in the ASI. These transactions may be declined by Issuers. The Merchant has included the AAV in the first authorization message.

Merchants. In such use cases there is one authentication but multiple authorizations, one for each of the Merchants.

Global requirement: The AAVs in both authorizations are the same and must match the AAV in the authentication.

Void original authorization and reauthorize use case: if an authorization response times out and another authorization is sent for the same transaction, then the AAV from the authentication linked to that transaction should be used.

To avoid expired authorizations, Merchants have to perform pre-authorizations/incremental authorizations to extend the validity period using the Trace ID.

European requirement: Merchant name—For the agent model, the authentication and purchase is made on a combined site (like a combined travel booking of airline and hotel) but the authorizations are for separate Merchants.

The booking agent must use the Merchant name, acquirer BIN and merchant ID as registered by the Acquirer of the merchant during authentication. Until that logic is possible, the booking agent can use their own name as Merchant name in authentication.

The Merchant has to use "booking agent merchant name" in the authorization Merchant name field. Until that logic is possible, the Merchant can use their Merchant name in authorization (the Merchant may not be aware that this is a multi-merchant booking).

If and when needed, the Merchant can initiate an authentication request that, when referring to the (SCA) authentication request of the agent, could be managed as an MIT (provided the Cardholder gave a mandate to this end).

NOTE: The name in clearing can be different and should not be changed to comply with current rules.

European recommendation for dynamic linking: It is recommended that Merchant names in the clearing message contains the agent name and a reference to the individual Merchant(s) of the different transactions so that the transaction can be easily recognized by the Cardholder and dispute resolution is not initiated for transactions not recognized by the Cardholder.

Unknown/Undefined Final Amount Before Purchase

This is a use case when for example, payments are made on a travel turnstile or when fines are assessed after days/months of car rental. This includes as well examples of groceries where fruits and vegetables are charged per weight or when an ordered item is replaced by a more expensive item.

In such use cases, the Merchant sends an authentication request for the pre-agreed purchase amount plus the typical margin in business.

Global recommendation: If the final transaction amount is higher, then it is recommended that an authentication request be made for the incremental amount.

European recommendation for dynamic linking: The amount in the authentication (pre-agreed purchase amount plus the typical margin in business) will need to be clearly communicated to the Cardholder. The Merchant should display, during checkout, the message

"The Authentication amount has been raised to … to include a margin. This amount has no financial impact on your card account" (or similar) to avoid Cardholder confusion and abandonments.

The safety margin should be minimal to prevent the abandonment of the authentication experience in case the incremental amount is prohibitive.

Use Cases for Off-session Payments

Off-Session Payments are conducted when the Cardholder is NOT available behind his device to perform SCA.

This includes:

- Recurrent Payment with fixed amounts
- Recurrent Payment with variable amounts
- Recurring Payment combined with one-time purchase (mixed cart)
- Recurring payment with fixed limit/threshold (individual or corporate)
- Modifiable basket until cut-off
- Decoupled authentication

Recurring Payments

Global requirement: A Recurring Payment shall be indicated by the Merchant by the existing value 02 (=Recurring transaction) in the existing 3DS Requestor Authentication Indicator of the Authentication Request (AReq).

Global recommendation: A Strong Customer Authentication (SCA) for the first transaction of the recurring payments. If SCA is used based on the recommendation above, the 3DS Requestor Challenge Indicator = "04".

Global recommendation: Recurring payments with a variable frequency can set the Recurring Frequency to "1" to indicate that the frequency of payments is not set.

Mastercard's Position for Europe

Effective 18 October 2019 for intra-EEA recurring payment transactions, acquirers must provide the unique Trace ID of the initial recurring payment authorization in DE 48, subelement 63 (Trace ID) of subsequent recurring payment transaction authorizations to allow the issuer to validate that SCA occurred on the initial recurring payment authorization, as is required under PSD2 RTS.

NOTE: Refer to *Mastercard Rules* for the latest information on this topic. During soft enforcement of the PSD2 SCA regulation, temporary non compliance that this latter regulation is tolerated if a migration plan has been approved by the National Competent Authorities until the applicable grace period ends.

This rule does not apply to reversals, which must continue to include the Trace ID of the authorization to be reversed. Refer to release announcement *AN 2630—Use of Trace ID to Support PSD2 Recurring Payment Requirements* for more details.

If the initial authorization happened before 14 September 2019 and the initial Trace ID is not available (for example, was not stored), or if the recurring payment was set-up via mail order, telephone order, or via face-to-face and the initial Trace ID is not available, then the Trace ID must have the following values:

- Positions 1–3 = value "MCC" for Mastercard Card
- Positions 4–9 = value "999999"
- Positions 10–13 = value "1231"
- Positions 14–15 = blank filled

Alternatively, if the initial authorization happened before 14 September 2019, then the Trace ID can refer to any other authorization belonging to that same recurring payment arrangement provided this authorization took place before 14 September 2019.

Effective 14 September 2019, the Issuer is recommended to be able to store the Trace ID so that it is able to validate that SCA that took place when setting up the recurring payment arrangement. This Trace ID will be considered as the reference to the mandate that the cardholder provided to and authenticated with the merchant.

Effective 18 October 2019, EEA Issuers must be able to process the Trace ID provided in authorizations in DE 48 sub-element 63 (Trace ID), for example to validate if an initial SCA took place to set-up the recurring payment arrangement as required under PSD2 RTS. As this is an existing data element in authorization, it can be used before.

Effective 14 September 2019, for remote electronic transactions effected in the EEA, the transactions in a series of recurring payment transactions will require:

- That the initial authorization must be flagged as a recurring payment
  - DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence) has a value of 4 (Standing order/recurring transactions),
  - As result of the SCA requirement, DE 48, subfield 42 (Electronic Commerce Indicators) Security Level Indicator = 212, and
  - As result of the SCA requirement, DE 48, subfield 43 (Universal Cardholder Authentication Field [UCAF])) = Accountholder Authentication Value (AAV) with leading indicator kH or kB,
  - But without DE 48, subfield 63 (as no previous Trace ID is available)
- That subsequent authorizations are flagged as recurring payments
  - DE 61, subfield 4 (POS Cardholder Presence) has a value of 4 (Standing order/recurring transactions), and

– With the Trace ID in DE 48 subfield 63

European requirement for dynamic linking:

For existing Recurring Payments at the PSD2 RTS effective date of 14th September 2019, for example Recurring Payments setup before this date, the principle of "grandfathering" is applied. This means that SCA is applicable to the setup of new Recurring Payments only, for example, Recurring Payments initiated after the effective date of 14th September 2019.

Grandfathered Recurring Payments are indicated as follows:

- 3DS Requestor Prior Transaction Reference = DS Transaction ID of the initial Recurring Payment Agreement authentication. This reference is a must to complete the authentication process successfully. All nines ("9") if the agreement was concluded before 14th September 2019.
- DE 48 SE 63 = Trace ID of the initial Recurring Payment Agreement. This reference is a must to complete the authentication process successfully. The Trace ID includes the Banknet Reference Number (BRN). The BRN will be set to "999999" if the agreement was concluded before 14th September 2019[7].

[7] In between 14th September and 1st November 2019, Issuer shall not decline recurring payment transactions just because the TraceID is absent: it is recommended to consider subsequent recurring payments as grandfathered.

Recurring Payment and MIT for Recurring Payments—Initial Transaction

The following tables indicate the flags to be used for Recurring Payments in the authentication and authorization for the initial transaction in the series and for subsequent ones.

Table 1: Recurring Payment and MIT for Recurring Payments—Initial Transaction

Authentication	Authorization
• **Channel = PA (Payment Authentication)** • *3DS Requestor Authentication Indicator*= "02" (Recurring Payment) • **3DS *Requestor Challenge Indicator* = "03" (Challenge requested: 3DS Requestor Preference) or "04" (Challenge requested: Mandate). "04" for regulated markets.** • ***3DS Requestor Prior Transaction Reference* = {empty}** • ***Purchase Amount* = Maximum amount of the Recurring Payment Agreement or zero** • *Recurring Expiry* = Date at which Recurring Payment Agreement needs re- authentication • *Recurring Frequency* = Frequency of the Recurring Payment Agreement (1 when no frequency is set) DS Outcome: DS Transaction ID and AAV	• **DE 4 (Transaction Amount) = Authenticated Purchase Amount** • DE 22 (POS Entry Mode) = "10" (Card on File) or "81" if card details entered for the first time • **DE 48 SE 22 SF 1 not set.** • **DE 48 SE 42 = 212 or 217** • DE 48 SE 43 = AAV from authentication (SLI 212) • **DE48SE63 = {empty}** • DE 48 SE 66 SF 1 = "2" (EMV 3–D Secure [3DS 2.X]) • DE 48 SE 66 SF 2 = DS Transaction ID from authentication • DE 61 SE 4 = "4" (Standing order/recurring transactions) Authorization Outcome: Trace ID

NOTE: Bold text highlights items changing between the first transaction and subsequent ones.

Table 2: Recurring Payment and MIT for Recurring Payments—Subsequent Transactions

Authentication (optional)	Authorization
• **Channel = 3RI to indicate the cardholder is off-session as from EMV 3DS 2.2 only. Not available in EMV 3DS 2.1.** Issuers must skip AAV validation if the 3DS Requestor Prior Transaction Reference links to the initial Recurring Payment or MIT Agreement. • *3DS Requestor Authentication Indicator*="02" (Recurring Payment) • ***3DS Requestor Challenge Indicator* = "5" (Acquirer exemption)** • ***3DS Requestor Prior Transaction Reference* = DS Transaction ID for initial Recurring Payment Agreement authentication. All nines (9) if before 14 September 2019.** • ***Purchase Amount* = Amount not higher than the initial agreement Purchase Amount** • *Recurring Expiry* = Date at which Recurring Payment Agreement needs re-authentication • *Recurring Frequency* = Frequency of the Recurring Payment Agreement (1 when no frequency is set)	• **DE 4 (Transaction Amount) = Purchase Amount (not higher than the initial agreement Purchase Amount)** • DE 22 = "10" (Card on File) or "81" if card details entered for the first time • **DE 48 SE 22 SF 1= "03" (Recurring Payment Exemption) or "01" (MIT)** • **DE 48 SE 42 = 212 or 217 (Fully authenticated if Issuer RBA has been used) or 210 (if no subsequent authentication or Acquirer Exemption/MIT). 216 if subsequent authentication and Recurring Payment was requested with Acquirer Exemption or MIT** • DE 48 SE 43 = AAV from authentication (SLI 212 or 216) • **DE 48 SE 63=Trace ID of initial Recurring Payment Agreement. "999999" as Banknet Reference Number if before 14 September 2019.** [8] • DE 48 SE 66 SF 1 = "2" (EMV 3–D Secure (3DS 2.X) (SLI 212 or 216) • DE 48 SE 66 SF 2 = DS Transaction ID from authentication (SLI 212 or 216) • DE 61 SE 4 = "4" (Standing order/recurring transactions). This applies as well to all MITs, including the industry specific ones (such as, hotel no show, fines post car rental).

NOTE: Bold text highlights items changing between the first transaction and subsequent ones.

Installments

EMV 3DS specifications considers Installments as a special case of Recurring Payment where the amount and frequency are fixed and limited in time (Recurring Frequency not set to "1").

Such specification does not align with the Mastercard Rules where Installments must have following characteristics:

[8] In between 14th September and 1st November 2019, Issuer shall not decline recurring payment transactions just because the Trace ID is absent: it is recommended to consider subsequent recurring payments as grandfathered.

- Authorization must be unique and for the full amount of the transaction. Issuers need to manage the open-to-buy of cardholders taking the installments into account.
- Clearing occurs per installment payment

Consequently, the amount of the authentication will be the total amount of the purchase or sum of all installments, including fees and interest.

Decoupled Authentication

This section is provided for information only. The decoupled authentication feature is not yet available. Mastercard will communicate in future announcements when this feature can be used.

It may happen that, in a challenge situation, Issuers want to reach out to authenticate their Cardholder outside of the EMV 3DS message flows. Use cases are:

- Where SCA may be required when the Cardholder is off- session (recurring payments for variable amounts, authorization amount is above authentication amount and an authentication for the difference is needed).
- For Mail Order/Telephone Order (MOTO) transactions. Refer to section Mail Order/ Telephone Order (MOTO).

The EMV 3DS 2.2 specifications support decoupled authentications.

In a typical decoupled authentication, the following flow will apply:

- The Merchant initiates an Authentication Request (AReq) indicating they would like to perform a decoupled authentication with the maximum timeout allowed for example, 1 week).
- The Issuer responds back indicating they support decoupled authentication for their Cardholders or not.
- If this Issuer does, it authenticates the Cardholder outside the normal Challenge Request/ Challenge Response (CReq/Cres) flow.
- Upon authentication, the Issuer sends the results back via the Results Request (RReq) message
- The Merchant confirms with the Results Response (RRes).

Before the authentication window times out, the recommended user experience is for Issuers to attempt strong customer authentication via authentication app with push notification or email. Several attempts may be required in the allowed authentication window.

As the Cardholder will be off-session and the authentication will be decoupled, it is important that the Cardholder is given all necessary recognizable data elements (Merchant name, incremental transaction amount, reasons for additional authentication) that will allow him to go through the authentication process seamlessly.

Chapter 5 General Principles for Travel Sector

This chapter covers general principles for applying SCA in specific Travel Sector use cases. Refer to the Appendix E of this document for further details on the Travel Sector.

Merchant Category Codes (MCCs)

There are Merchant Category Codes (MCCs) that can be used for the identification of the Travel and Hospitality sector.

- Airlines and Air Carriers: MCCs 3000 through 3350 and MCC 4511
- Lodging: MCCs 3501 through 3999 and MCC 7011
- Car Rentals: MCCs 3351 through 3500 and MCC 7512
- Cruise Lines: MCC 4411
- Travel Agencies: MCC 4722
- Railways: MCC 4112
- Bus Lines: MCC 4131

Application of Merchant Initiated Transaction (MIT) Exclusion

A MIT agreement can be created between the Merchant and the Cardholder in cases where there may be multiple payments and/or when one or more of the payment authorizations are likely to occur after the AAV retention period (90 days).

Refer to section Merchant-Initiated Transactions.

To ensure a MIT meets the EBA requirements, Mastercard suggests any agreement includes the following:

- Name and full address of Merchant
- Purpose of the agreement / payment
- Type of payment (such as, recurring, one-off)
- Duration of the agreement
- Total amount and currency of the agreement (or an estimate if the precise payment amount is not known)
- Amount and currency of the authentication
- Amount and currency of the first payment
- Cancellation procedure
- Payment schedule and/or timing of first payment

Mastercard also strongly recommends that the Merchant confirms all components of the MIT agreement with the consumer via email.

- Within the travel and hospitality sector, MIT agreements are comprised of those:
  - Set up by the Travel Agent with partial payments collected by the Travel Agent and the Travel Supplier. For example, a Travel Agent that collects payments for their fees, and passes the traveler's card details to the Travel Supplier (such as, airline), makes a separate charge on the card for the services hired.
  - Set up by the Travel Agent with partial payments collected by the Travel Supplier only. For example, when an Travel Agency organizes a booking for a Hotel stay, passes the

traveler's card details to a Travel Supplier and the Travel Supplier makes partial charges on the traveler's card (such as, reservation deposit, first night payment)
  - Combination of the above in a multi-Merchant use case
- Examples of MIT Use Cases in Travel Sector:
  - Additional charges added to the initially agreed amount
    (Example Use Case: Additional mini-bar expenses of €50 charged by hotel at checkout or fines associated with a rental car agreement)
  - Transactions separated into different payments occurring at different times such as installments or deposits for travel bookings
    (Example Use Case: Tour Operator booking with a deposit to secure the booking. Value of booking: €2,000: Initial deposit of €50 collected at time of booking followed by 3 monthly payments of €650)
- Under PSD2 guidelines, if a transaction is designated a MIT, SCA is applied on the first payment when setting up the MIT with the Cardholder (such as, during booking), and the subsequent authorization allows the Issuer to confirm the agreement. The Trace ID becomes the unique reference of the approved agreement.
- Subsequent payment authorizations related to the MIT agreement do not require SCA, but should include the original Trace ID and MIT flag.
- The Issuer bears liability on the initial authorization if 3DS has been used, but liability shifts to the Merchant for subsequent Merchant Initiated Transactions as these do not use 3DS.
- It is required that the Merchant initiates an authorization within the validity period of the Accountholder Authentication Value (AAV) in order to obtain a Trace ID that can be presented with subsequent authorizations. Under current Mastercard rules, the AAV validity period is set to 90 days. This means the Merchant processes the initial authentication and may retain the AAV for 90 days. Correspondingly, the Issuer must approve the authentication value within 90 days.
- If the Merchant attempts to use an AAV that has expired (such as, Merchant attempts to use an AAV on a booking made six months in advance), the issuer may decline the transaction.
- For Recurring transactions/MITs, subsequent transactions cannot use the AAV, but must carry the initial authorization's Trace ID.
- Mastercard is considering allowing Merchants to request an extension for the AAV by sending a 3RI request before expiration of the 90 days retention period in the future, but no determination has been made at this time.

Mastercard's Position for Europe

Mastercard requires that MIT authentications should be identified using the appropriate flag in order to deter the Issuer from stepping up the transaction (see Merchant-Initiated Transaction (MIT) for list of 3DS indicator fields).

The EMV 3DS specification supporting MITs are 3DS Requester Challenge Indicator "02" and PSD2 Mastercard Message Extension Field1 "Acquirer SCA exemption" = "05" / No challenge requested (TRA already performed).

Issuers are instructed not to automatically decline MIT authorizations without 3DS and to not step-up unless high risk if EMV 3DS is used.

The authorization (including zero amount account status inquiry messages) that follows the MIT agreement should carry the AAV and does include Issuer liability. Merchants are advised to collect a first payment during this initial authorization so that they can benefit from the liability shift. It is also recommended that, if the amount is not known up front, the Merchant uses the same first payment amount value in the initial authentication.

If the payment is centralized, the Travel Agent processes the transactions centrally via a single provider. If the payment is not centralized, the Travel Agent shares the payment detail with the Travel Supplier(s). The Travel Supplier then processes the payment authorization.

Mail Order/Telephone Order (MOTO) and Manual PAN Key Entry

Mastercard requires that Merchants identify transactions booked through mail or telephone channels as MOTO, which are a type of card not present transactions. MOTO transactions are of out scope for PSD2 RTS and can be passed directly to authorization without authentication.

MOTO transactions are identified in DE 61 SF 4 by a value of 2 (CNP - mail/facsimile) or 3 (CNP-phone or automated response unit) in DE 62 SF 4. The Merchant or PSP/Acquirer are responsible for flagging MOTO transactions correctly.

PAN Key Entry transactions are also typically a type of Card Not Present (CNP) transactions. PAN Key Entry transactions are common in the travel industry (such as, hotel segment) and may not correctly reflect the booking method which could be either online, MOTO or other channels. Consequently, terminals may or may not be initiating transactions that are in scope of PSD2 RTS.

PSP/Acquirer are responsible for correctly reflecting the booking method. Mastercard recognizes the fact that PSP/Acquirers are in the process of updating systems to reflect manual PAN Key Entry transactions correctly and therefore recommends Issuers to not systematically decline these transactions. Mastercard recommends Travel Agents and Service Providers in the travel industry to build appropriate channels to share the authentication data down to the payment authorization to ensure that properly flagged transactions can be presented.

- If the Merchant (such as, Travel Supplier) is aware that the booking occurred through telephone or mail then the transaction must be flagged as MOTO.
- Mastercard recommends that Issuers do not systematically decline POS-EM "01" PAN Key Entry with POS-CC "CNP" as these can be considered MOTO.
- Mastercard also recommends that the Travel Agent/Service Provider to share the authentication details to allow a standard CNP authorization to be initiated. Authentication details including protocol version, DS Transaction ID, SLI, exemptions requested and AAV would need to be passed.
- The use case can also be applied to multiple Merchants as the same AAV can be shared with multiple Merchants if a single authentication is related to multiple transactions.

- Mastercard recommends the travel sector to ensure that transactions are properly flagged and that the authentication information, when booking occurred online, can be channeled securely from the Merchant into the payment authorization.

Authentication

Whenever reservations are being made online and authenticated (with or without application of exemptions), subsequent payment authorizations need to reflect the remote (card-not-present) transaction type with identification of the authentication and/or the exemptions that may have been applied.

Amount in Authentication and Authorization

The following considerations apply to amounts to be used in authentication and authorization.

- Payment Amount: Mastercard guidelines allow for payment authentication amounts to be greater than or equal to authorization amount
  - If the full amount is being paid upfront (such as, airline ticket) then the total amount of the ticket should be authenticated.
  - If a booking/travel agent is managing the transaction, it is recommended the agent authenticate for the total amount of the booking. Mastercard recommends that all policies related to cancellation and timing of charges be included in the T&Cs and shared with the cardholder upfront before authorizing the agent to make transactions.
- Currency: Mastercard has determined that payment currency must be the same for both authentication and authorization
- Unknown Payment Amount: If the final payment amount is not known at the time of the booking, Mastercard advises using an amount that may meet reasonable customer expectations (we believe that an average of 20 percent tolerance should be allowed - if above 20 percent additional authentication may be required).
- MIT Agreements: A MIT agreement may involve multiple payments not known at the time of booking. In this case the following should be considered:
  - If the total amount of the agreement is known up front, it should be mentioned in the agreement and used as the amount of the authentication
  - If the total amount is not known upfront, it is recommended for the authentication amount used for the agreement to match the first payment authorization amount
  - If the first or total payment cannot be determined at the time of authentication, a zero authentication amount can be used. In such case a zero authorization amount through an Account Status Inquiry message can be used for the Issuer to confirm the agreement. (Example: Hotel reservation made without an initial payment that may include charges from the restaurant before the AAV expires.)

Merchant Location

Merchant Location is defined as where the Merchant conducts business and operations, holds a permit to operate the business, complies with tax laws and regulations and is subject to consumer laws and courts.

The Merchant Location is identified through Merchant Country in authentication and authorization.

PSD2 RTS Geographical Scope:

- PSD2 RTS geographical scope is based on Issuer and Acquirer location. Even when the Merchant Location is outside of EEA, an Acquirer in EEA requires the Issuer to apply SCA.
- Non-EEA Merchants are required to share the EEA Acquirer Country Code in the authentication. This is not a requirement for EEA Merchants.
- In a two-leg transaction, if both the Issuer and Acquirer are within the EU (EEA), then the PSD2 RTS apply.
- When the Merchant's Acquirer is not known at time of booking (authentication and/or authorization), the following should be considered:
  - There are use cases where the Travel Agent/GDS/Service Provider is authenticating the transaction but is not the MoR and may not know the MoR's Acquirer nor Merchant Location.
  - In these instances the Travel Agent/GDS/Service Provider must identify a Merchant Location and if appropriate an Acquirer Location that respects the EEA geographic location even if it is not the correct Merchant or Acquirer country.
    During authentication, for EEA Merchants, Issuers are recommended to use the Merchant Location as proxy and disregard the Acquirer Location.
  - The Merchant then submits the authorization with the correct Merchant and Acquirer Location.
    - For those airline transactions that are authorized by the GDS, the GDS must then submit the authorization with the corresponding Merchant Location as identified in the authentication
      During authorization, for EEA Merchants, Issuers are recommended to use the Merchant Location as a proxy and disregard the Acquirer Location.
    - Ultimately the clearing contains the correct Merchant and Acquirer Location.

As part of the EMV 3DS 2.1 message extension the Acquirer Country Code is allowed to be shared with the Issuer. The field is optional but must be provided when the Merchant is not in the EEA, whereas the Acquirer is in the EEA. The data in the authorization is not carried but it can be deducted from the Acquirer BIN in the transaction.

Merchant Identification

A Merchant is identified through the identifier couple Acquirer BIN-Merchant ID (MID) and reflects the Merchant as it has been registered (through ISSM) by the Acquirer.

As much as possible, the Merchant Identification must be consistent between authentication and authorization.

- There are use cases where the Travel Agent/GDS/Service Provider is authenticating the transaction but is not authenticating the MoR and may not know the Merchant of Record's Acquirer BIN nor Merchant ID. This is a frequent use case with Travel Agents and GDS supporting the booking.
- In these instances where the Acquirer is not known, those Travel Agent/GDS/Service Provider may be using Acquirer BINs and MIDs in the authentication that do not belong to or have not been registered by the Merchant of Record's Acquirer. It is still required that the Acquirer BIN-Merchant ID are registered by the entity requesting the authentication
  - For the airline transactions that are authorized by a GDS, the GDS uses their own Acquirer BIN and MID to pass the transaction into authorization. As this is a current practice, again this Acquirer BIN and MID are not reflecting the Merchant of Record's Acquirer
  - Ultimately the clearing must contain the correct Acquirer BIN and Acquirer registered MID

Multi-Merchant Bookings

Multi-Merchant bookings include those direct or indirect sales in which a customer books several travel services through the same Travel Agency or Service Provider Entity.

Example: Travel Agent offers a vacation package combining airline, hotel and car rental bookings.

- MIT agreements can also be established for multi-Merchant transactions
- In the event that a single reservation involves multiple merchants (such as, holiday package), the Travel Agent must be identified as the Merchant of Record in the authentication. Subsequent payment authorizations must reflect agent and merchant name separated by "*" (for example, TravelAgent*Merchant),
- For the multi-Merchant use case, the same authentication code/AAV can be used in accordance with current PSD2 guidelines
- An authentication performed for a booking at an agent involving multiple Merchants must have an authentication amount that equals the total of the individual payment amounts
- If one or more of these Merchants are covered with an MIT agreement set up by the booking agent then the total authentication amount must reflect the sum of the individual MIT agreements for which the same amount specifications apply as for a single-Merchant MIT agreement

The following table outlines the recommended technical approach to be undertaken and flags to be used for the above listed travel sector general principles.

General Principle		Comments
MIT Exclusion	An MIT agreement can be agreed between a consumer and a Merchant in cases where there are multiple payments and/or when one or more of the payment authorizations are likely to occur after the AAV retention period (90 days).	An MIT Agreement does not supersede Law nor Mastercard Rules. **SCA at agreement set up (first transaction in a series)** The subsequent authorization allows the Issuer to confirm the agreement • The TraceID (authorization DE63) becomes the unique reference of the approved agreement. • This authorization can be an Account Status Inquiry message (authorization DE 61 SF 7 = 8) with zero transaction amount. **Subsequent payment authorizations** require: • the Original TraceID in the authorization DE 48 SE 63. • the MIT flag (authorization DE 48 SE 22 SF 1 = "01).

General Principle		Comments
PAN Key Entry and MOTO	PAN Key Entry transactions (authorization DE 22 SF 1 = "01") typically are of a "card not present" transaction type and can be considered as remote transactions. MOTO transactions (authorization DE 61 SF 4 = "3" or "4") are also a flavor of "card not present" transactions.	PAN Key Entered transactions are very common in the hotel segment of the travel industry and may not always correctly reflect the booking method; either on-line, MOTO or other channels. Consequently these terminals may or may not be initiating transactions that are in scope of PSD2 RTS. Authentication information, when booking occurred on-line, must be channeled securely to the Merchant. This ensures that the Merchant Acquirer can properly flag these transactions into the payment authorization message. Until the travel industry stakeholders have implemented the required changes, Mastercard recommends Issuers not to systematically decline such PAN Key Entry authorizations Reservations that have been made through mail or telephone order for which no authentication is required need to be flagged as MOTO in subsequent payment authorizations (MOTO is out of PSD2 RTS scope and does not require SCA).

General Principle		Comments
Authentication - AAV	The Authentication Value retention period is 90 days. Merchants must ensure to have the authentication value approved by the Issuer before expiration of the retention period. When there is a risk that the payment (clearing) may occur later than the authorization life cycle period (30 days for credit, 7 days for debit) then either a pre-authorization or an MIT Agreement may need to be considered.	Merchants or their Agent need to be aware of the time frame characteristics of the travel industry: • When the payment clearing occurs within the authorization life cycle (30 days for credit, 7 days for debit) then the AAV is presented to the Issuer for approval at the time of the payment authorization. • When the payment clearing occurs outside the initial authorization life cycle but before the AAV retention period expires, then the AAV must be presented to the Issuer for approval during the initial payment pre-authorization. – Subsequent (pre-) authorization must then use Trace ID (authorization DE 48 SE 63) of the initial pre-authorization. When the payment clearing occurs outside the AAV retention period then AAV must be presented to the Issuer for approval in a (pre-) authorization or Account Status Inquiry message (authorization DE 61 SF 7 = 8) before expiration of the AAV retention period.

General Principle		Comments
Amount in Authentication and Authorization	The authentication amount (authentication purchaseAmount) and currency (authentication purchaseCurrency) must match the authorization amount (authorization DE 4) and currency (authorization DE 49).	**Exception: MIT Agreement** An MIT Agreement may involve multiple payments not known at the time of booking but subject to the agreement • Ideally, if the total amount of the agreement is known up front, it should be mentioned in the agreement and used as the amount of the authentication. • If the total amount is not known upfront, the authentication amount used for the agreement has to match the first payment authorization amount. • If first payment amount or even the total agreement amount cannot be determined at the time of authentication, a zero authentication amount has to be used. In such case a zero authorization amount through an Account Status Inquiry message (authorization DE 61 SF 7 = 8) has to be used for the Issuer to confirm the agreement.

General Principle		Comments
		Exception: Multi-Merchant booking An authentication performed by a Travel Agent for a booking involving multiple Merchants must have an authentication amount that equals the total of the individual payment amounts. If one or more of these Merchants are covered with an MIT agreement set up by the Travel Agent then the total authentication amount must reflect the sum of the individual MIT agreements for which the same amount specifications apply as for a Single-Merchant MIT Agreement.
Merchant Location	Merchant Location is defined as where the Merchant conducts business and operations, holds a permit to operate the business, complies with tax laws and regulations and is subject to consumer laws and courts. The Merchant location is identified through Merchant country in authentication (authentication MerchantCountryCode) and authorization (authorization DE 43 SF 5).	**Defining the correct PSD2 RTS geographical scope** An Issuer needs to determine PSD2 RTS geographical scope based on Acquirer location. Even when Merchant Location is outside of EEA, an Acquirer in EEA will require the Issuer to apply SCA. Non-EEA Merchants are required to share the EEA Acquirer Country Code in the authentication (Mastercard PSD2 Message Extension to EMV 3DS 2.1, Field 3). **When the Merchant Acquirer is not known at time of booking or payment** There are use cases where the booking agent is not the Merchant of Record and may not know the Merchant of Record's Acquirer nor Merchant location.

General Principle	Comments
	• In these instances those booking agents must be identifying a Merchant location and if appropriate an Acquirer location that respects the EEA geographic location even if it is not the correct Merchant or Acquirer country. During authentication, for EEA Merchants, Issuers are recommended to use the Merchant location as proxy and disregard the Acquirer location. • The authorization must then be submitted with the corresponding Merchant location as identified in the authentication. During authorization, for EEA Merchants, Issuers are recommended to use the Merchant location as proxy and disregard the Acquirer location. • Ultimately the clearing must contain the correct Merchant and Acquirer location.

General Principle		Comments
Merchant Identification – Merchant Name	The Merchant that sells the goods or services to the consumer needs to be reflected in the authentication (authentication MerchantName) and authorization (authorization DE 43 SF 1). As much as possible, the Merchant name must be consistent between authentication and authorization.	**Booking and payment managed by same entity** • When airlines, hotels are organizing the reservation/ booking and payment of their travel services they are Merchant of Record during a transaction and need to be identified as such in authentication and authorization. • When travel agent is organizing the reservation/ booking and payment of an airline, hotel or other travel provider service on behalf of this travel provider, the travel agent is Merchant of Record during a transaction and need to be identified as such in authentication and authorization.

General Principle		Comments
		Booking and payment managed by different entities • Ideally, when a third party such as a Travel Agency is organizing the reservation/ booking of an airline, hotel or other travel services on behalf of the Travel Supplier but the Travel Supplier is the one processing the payment, the Travel Supplier is considered the MoR and needs to be identified as such in authentication and authorization. Ad interim and until the infrastructure is updated, travel agents are allowed to use their name as merchant name. • In case multiple Merchants are being included in one single reservation by the Agent (for example, in a package) then the Agent must be identified as the Merchant of Record in the authentication. – Subsequent payment authorizations must reflect agent and Merchant name separated by "*" (for example, TravelAgent*Airline)
Merchant Identification – Merchant of Record	A Merchant is identified through the identifier couple Acquirer BIN-Merchant ID (MID) and reflects the Merchant as it has been registered (through ISSM) by the Acquirer. As much as possible, the Merchant identification must be consistent between authentication and authorization.	There are use cases where the Travel Agent / GDS / Service Provider is authenticating the transaction but are not the Merchant of Record and may not know the Merchant of Record's Acquirer (BIN) nor Merchant (MID). This is a frequent use case in the airline business but may also occur in other travel segments.

General Principle	Comments
	• In these instances those Travel Agents/GDS/Service Providers may be using Acquirer BINs and MIDs in the authentication that do not belong to or have not been registered by the Merchant's Acquirer. It still is required that the Acquirer BIN-Merchant ID are registered by the entity requesting the authentication. • Subsequently and specific to airline travel, a GDS may then be using their own Acquirer BIN and MID to pass the transaction into authorization. Again this Acquirer BIN and MID are not reflecting the Merchant's Acquirer. • Ultimately the clearing must contain the correct Acquirer BIN and Acquirer registered MID.

Chapter 6 Specific Requirements Under PSD2

This section contains information on when to apply to SCA, dynamic linking requirements and AAV validation, fraud level calculation, and transaction monitoring.

When to Apply SCA

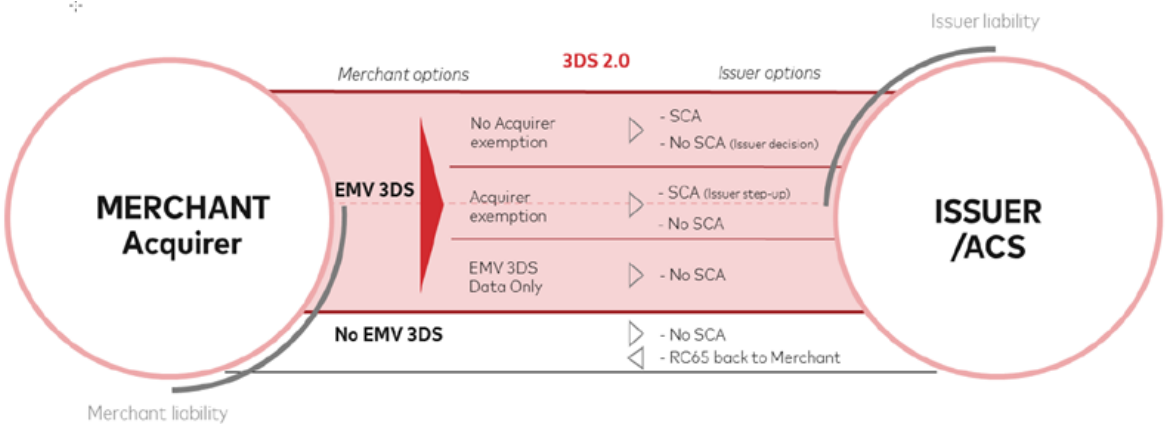
SCA needs to be applied as per PSD2 RTS requirements.

SCA is required when:

- The transaction is not out of scope of the PSD2 RTS
- No PSD2 SCA exemption applies for a payment transaction
- Adding a card to a Merchant's file (card-on-file)
- Starting a recurring payment arrangement for fixed and variable amounts, including Merchant-Initiated Transactions
- Changing a recurring payment agreement for a higher amount (premium offering for example)
- White-listing (or viewing/amending white-lists)
- Binding a device to a Cardholder

In all other scenarios the Issuer always has the final word to apply SCA. Mastercard recommends that, risk permitting, Issuers offer a frictionless consumer experience when SCA is not required by regulation.

Mastercard offers all possible authentication combinations to satisfy Issuers and Acquirers needs. The following diagram depicts options available at the Merchant side as well as at the Issuer side, compatible options as well as where liability lies under PSD2 RTS requirements.



In the case of Whitelisting, the Merchant does not know in advance if it is Whitelisted (or if it has been removed from the Cardholder's Merchant white list). The Merchant should therefore systematically initiate the EMV 3DS flow as if SCA would apply.

Dynamic Linking Requirements and AAV Validation

The Merchant name and authentication amount have to be shown to the Cardholder during the authentication experience, on the Merchant page (controlled by the 3DS Server) and on the authentication page (controlled by the ACS).

The information is available in the EMV 3DS AReq message with MerchantName and purchaseAmount.

Dynamic Linking is required: the authentication code (AAV) has to be linked to the Merchant and authentication amount.

As suggested by the EBA Opinion, effective 20 December 2020, the dynamic linking requirement is met if the Merchant is identified by its IBAN or another "unique identifier". The Merchant and its name in clearing can be different and should not be changed to comply with current rules.

NOTE: The initial SCA for MIT mandate is not subject to the dynamic link requirement. This is because the initial mandate is an "action through a remote channel, which may imply a risk of payment fraud or other abuses" under Article 97(1)(c) PSD2. The dynamic link requirement does not apply to these actions.

Mastercard is aware that current business and industry practices do not always allow for such linking of the merchant name and amount. On the Merchant name alone, there are cases where the Merchant is never the same in authentication and authorization:

- when a single authentication is used for multiple authorizations each with a different Merchant, for example, travel bookings and market places;
- when it is very difficult to use the same Merchant, for example, when different Acquirers are used for authentication and authorization.

The Mastercard on-behalf AAV validation service compares the PAN, the amount, the DS Transaction ID, and the SPA2 AAV in authentication and authorization. By comparing multiple data points in authentication and authorization, Mastercard uniquely identifies the transaction and, consequently, ensures that the merchant identity is the same throughout the payment flow. Mastercard does not directly match on merchant name due to significant mismatch risk in case of, for example, marketplace purchases with several suppliers executing the order following a single authentication (in December 2019 around 30 percent of all EMV 3DS transactions used a different merchant name in authentication and authorization). The European Banking Authority (EBA) clarified through its Q&A tool (Q&A 2019_4556 of December 20, 2019) that the PSD2 RTS requirements for dynamic linking do not specify how the merchant should be identified. This means that dynamic linking can be complied with using other data than merchant name (or merchant ID).

Mastercard protects the AAV from interception and hence fraudulent use by encrypting it, transporting it over a secure private network, requiring storage on PCI DSS certified platforms and only for the minimum amount of time needed until the transaction is cleared and settled. By requiring not only the AAV to match, but also the DS Transaction ID, Mastercard believes

that this AAV validation service protects against card fraud in a superior way, ensures that the authentication code (AAV) is specific to the transaction authenticated by the cardholder and hence complies with PSD2 RTS requirements for dynamic linking.

The Mastercard On-Behalf AAV Validation Service performs AAV validation based on the DS Transaction ID and also informs the issuer how the amount in the authorization compares to the amount in the authentication (lower or the same, higher by up to 20 percent, higher than 20 percent).

The Mastercard fallback validation prevents fraud such as man-in-the-middle attacks by:

- comparing multiple data points in authentication and authorization (such as, PAN, DS Transaction ID, AAV, amount);
- storing such data in PCI DSS compliant sites; and
- transporting the data in a private secured network like the Mastercard network.

Re-using AAVs for fraudulent transactions becomes practically impossible.

Mastercard advises that for Issuers who perform AAV validation on their side, to recognize that if the AAV contains Merchant name and amount, these elements may cause the AAV validation to fail due to differences in these items between authentication and authorization. Therefore, Issuers are strongly recommended to use the SPA 2 AAV Validation method (refer to the *SPA2 AAV for the Mastercard Identity Check Program* manual) based on DS Transaction ID combined with a validation of the amount as the main reference and not based on Merchant name.

Mastercard advises Issuers to validate the dynamic linking based on the following process to avoid substantial declines of otherwise valid transactions:

1. During authentication, a unique DS Transaction ID is generated by Mastercard and provided to both Issuer's ACS and the Merchant. The Issuer's ACS generates an AAV cryptogram to confirm that the authentication was successfully performed.
2. The Merchant provides the DS Transaction ID with the AAV in the authorization message.
3. Self-validation by the Issuer: The Issuer self-validates Dynamic Linking during authorization processing using the following recommended approaches. The Issuer then calculates the part of the AAV called IAV using the same formula, method and encryption keys as originally calculated by the ACS:
    a. Option 1: ACS and Issuer calculate the IAV using the Merchant name and authorization amount provided respectively in the authentication and authorization message. The Issuer then compares the resulting IAV with the IAV provided in the authorization message as part of the AAV.
    If the IAV does not match, this could be due to the amounts and/or Merchant name being different from the authentication vs. authorization. In this case the Issuer needs to compare the amount and Merchant name from authentication to authorization and determine the potential variance between both.
    b. Option 2: both ACS and Issuer calculate the IAV using blanks for Merchant name and zeroes for the authorization amount. The Issuer then compares the resulting IAV with the IAV provided in the authorization message as part of the AAV.

If the IAV then does not match, this indicates that the IAV used in the authorization is likely not originating from the corresponding authentication message. If the IAV does match the Issuer needs to compare the amount and Merchant name from authentication to authorization and determine the potential variance between both.

c. Comparing the amount and Merchant name between authentication and authorization messages can be accomplished with the DS Transaction ID provided in the authorization message since it was also previously provided to the ACS during the authentication. It requires the Issuer's authorization system to have a direct real-time connection to the ACS to retrieve the authentication message that can then be compared to the authorization message.
An alternative to step c. is for Issuers to use the on-behalf AAV validation service offered by Mastercard. More details are provided in point 4 below.

d. When comparing the amount, the Issuer should also ensure that the authentication amount is not lower than the authorization amount, or the sum of the authorization amounts relating to the same DS Transaction ID.

e. Issuers cannot perform AAV validation with AAVs, which do not contain an IAV value. Issuers can determine which AAVs do not contain an IAV by reviewing the leading indicators (refer to the *SPA2 AAV for the Mastercard Identity Check Program* manual). Any leading indicator noting Mastercard (Smart Authentication) Stand-In Services are AAVs that Issuers cannot self-validate.

4. On-behalf AAV validation service by Mastercard.
Mastercard cannot validate the IAV. It is up to the Issuer to comply with the PSD2 RTS on SCA for dynamic linking. For example, Issuers may calculate the IAV based on the Primary Account Number (PAN), DS Transaction ID and amount. This requires the DS Transaction ID to be populated by the Acquirer, which explains why the DS Transaction ID is conditional, for example, mandated if the Acquirer is in the EEA.

   Self-validation by Issuers may be challenging for different reasons:

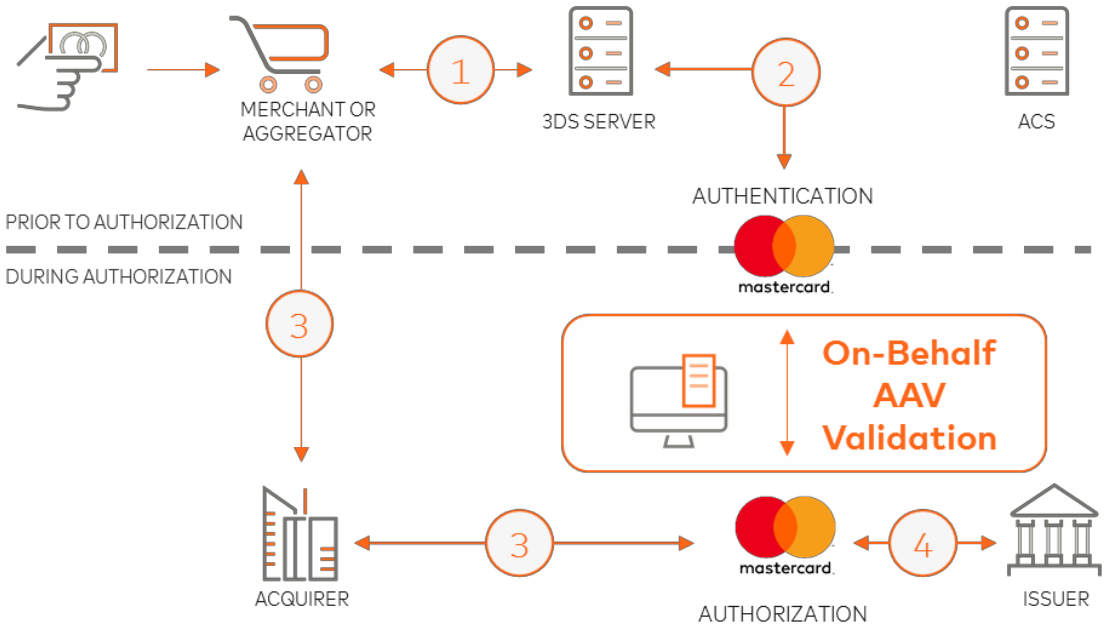
   – Different existing industry business and technical models make it from difficult to impossible to meet the requirement that the Merchant name and the amount in authentication and authorization must exactly match.
   – Issuers may experience delays in getting ready with EMV 3DS and PSD2 RTS due to complexity of the IAV validation and the requirement to exchange keys with their ACS.
   – Many Issuers do not have a real-time on-line connection to their ACS Service to access Authentication Data.

   Mastercard on-behalf AAV Validation Service can support Issuers due to:

   – Mastercard on-behalf AAV validation service is using its own keys and does not require any key exchange.
   – The Mastercard authentication and authorization networks are residing on connected platforms allowing easy and fast data matching and comparison.

   With the above argument in mind, Mastercard has suggested the following clarification to the PSD2 RTS on SCA:

"For remote transactions, if the transaction amount and/or the Merchant's name differs between authentication and authorization, the dynamic link requirement is complied with if the Issuer matches and validates the authentication cryptogram generated during authentication with the cryptogram sent in authorization."



The Mastercard on-behalf AAV validation service has been adapted so that:

Via the DS Transaction ID, Mastercard:

- Retrieves the AAV generated by the ACS during authentication and matches it to the AAV in the authorization message.
- Compares the authentication and authorization amounts.
- Provides the outcome of the above matching and comparison processes to the Issuer in the authorization message:
  - Match with lower or equal amount (result codes 'A' and 'V')
  - Match with amount with tolerance of less than 20 percent (result codes 'B' and 'S')
  - Match with amount with tolerance equal to 20 percent or above (result codes 'C' and 'T')
  - No Match (result codes 'D' and 'I')

  If the DS Transaction ID (despite a mandate to provide it) is not provided, then the on-behalf AAV validation attempts to match the authentication with the authorization based on the AAV and card number. The matching rate will be around 80 percent meaning that the validation is flagged as of lower quality.

Fraud Level Calculation

For the Mastercard Identity Check™ Program KPIs, target fraud rates will be reviewed annually based on program performance and may be adjusted to actual market needs throughout the program. Every Issuer must report its Mastercard fraud data to the Fraud and Loss Database.

For the PSD2 RTS, the methodology and any model used to calculate the fraud rates as well as the fraud rates themselves, shall be adequately documented and made fully available to the EBA and national competent authorities.

Refer to the RTS for the methodology and reporting requirements relating to RTS/SCA fraud rates as discussions are still ongoing. The following elements are considered:

- The fraud rate is based on electronic remote card-based payment transactions, for example, CNP transactions, in the EEA region (two-leg transactions) but excludes as per the PSD2 RTS:
  - Anonymous prepaid card transactions
  - Merchant-Initiated Transactions (MITs)
  - Mail Order/Telephone (MOTO) transactions
  - Friendly frauds
- Acquirer fraud data is provided by Mastercard through SAFE reports. SAFE reported data only includes fraud data for Mastercard branded cards. The breakdown of the information allows Acquirers to filter CNP minus MOTO transactions and get gross fraud rates.
- As suggested in the EBA Opinion document, gross fraud rates should be provided (for example, including fraud caused by an exemption applied by the other PSP). The fraud rate is the gross amount of fraudulent transactions meeting the above criteria divided by the gross amount of transactions meeting again the same above criteria.
- Refer to the Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2): "Guidelines on fraud reporting under Article 96(6) PSD2 (EBA-GL-2018-05)".
  Refer to the following document for more information on SAFE reports made available to Acquirers on a daily basis: *SAFE Product User Guide* available in the Publications section of Mastercard Connect™ for information on SAFE reported data and specifications.

As PSD2 RTS inevitably decreases fraud levels at the Issuer side, Issuer fraud prevention tools (neural, rule-based) should be retrained or be revisited (rules and thresholds) to accommodate the improved environment.

Key data elements needed for fraud reporting as per the EBA Fraud Guidelines can be found in various data elements. The following is a non-exhaustive list of those:

- Exemption type in DE 48, SE 22, SF 1;
- MIT flagging in DE 48, SE 22, SF 1;
- One-leg transactions based on the Acquirer country and Issuer country (see section on One-Leg Transactions);
- The link between the Fraud and Loss Database and authorization and clearing systems using the DS Transaction ID.

Fraud Types

Two fraud types in the Fraud and Loss Database comply with the PSD2 fraud types.

- Modification of payment details
- Manipulation of the Cardholder

The Fraud and Loss Database includes the DS Transaction ID and Program Protocol.

Transaction Monitoring

The PSD2 RTS' Article 2 specifies that Payment Service Providers (PSPs) shall have transaction monitoring mechanisms in place that enable them to detect unauthorized or fraudulent payment transactions.

Risk-based factors that should be taken into account include:

- lists of compromised or stolen authentication elements;
- the amount of each payment transaction;
- known fraud scenarios in the provision of payment services;
- signs of malware infection in any sessions of the authentication procedure;
- in case the access device or the software is provided by the PSP, a log of the use of the access device or the software provided to the Cardholder and the abnormal use of the access device or the software.

EMV 3DS with Transaction Monitoring data and solutions (including device data linked to fraud) will facilitate the compliance with the PSD2 RTS. Alternative technical solutions may also be used.

Chapter 7 Authentication Services

Mastercard offers Customers a number of authentication services to help them comply with the PSD2 RTS requirements.

Digital Transaction Insights

EMV 3DS allows ecommerce Merchants to share a wealth of Cardholder data that they may be collecting during the purchasing process. Through Authentication, Issuers may be taking the appropriate decision to challenge or authenticate based on a risk-based decision.

Mastercard Digital Transaction Insights enables Issuers to receive an assurance level assessment of this Cardholder data from Mastercard during the authorization process. By facilitating the exchange and normalization of consumer account and device data provided by participating Merchants in EMV 3DS, Mastercard Digital Transaction Insights helps give Issuers a level of assurance that consumers are transacting using attributes—such as account, device, and IP address, for example—that are typically associated with them.

It is recommended that these Digital Transaction Insights are used by the Issuer's fraud prevention tool to reduce fraud and false declines.

The Digital Transaction Insights service relies on the DS Transaction ID to match the authorization to the authentication. However, if the DS transaction ID is not provided, the service still performs the matching. In this latter case, the matching rate is around 80 percent.

The Digital Transaction Insights are delivered to an Issuer in two distinct fields:

- A risk assessment with a value from 0 to 9 (zero representing lowest risk)
- A reason code with a value from A to Z (A representing highest risk)

As Merchants coming on board of EMV 3DS are only expected to be fully migrated at the earliest by September 2019, Issuers should use this migration period to learn from the assessment and build fraud rules on the analysis results. Ad interim, Issuers may find the reason code most useful as it gives a concrete indication of the risk condition that is being identified.

Refer to the following document for more information on this topic: *AN 2122—Introduction of Mastercard Digital Transaction Insights Service*.

Smart Authentication for Issuer/ACS

The Smart Authentication for Issuer service previously known as ACS RBA, is available to Issuer's ACS services when receiving EMV 3DS authentication requests.

There may be instances where the Issuer's ACS services have limited to no risk scoring capabilities. For those Issuers, Mastercard provides a risk score in the authentication request towards the ACS service by applying a risk scoring model.

The ACS service is then able to apply the risk score in its authentication experience to determine whether or not an authentication challenge is required, for example to apply risk-based authentication.

This Risk Scoring for Authentication service is available for all European-regulated or non-regulated Issuers.

The Smart Authentication for Issuers risk assessment is delivered to an Issuer in three distinct fields:

- A risk assessment decision categorizing an authentication as low vs. not low risk
- A risk assessment with a value from 000 to 950 (zero representing lowest risk)
- A reason code with a value from A to Z (A representing highest risk)

ACS services may either use the risk assessment decision as input to their risk-based authentication process or they can use the risk assessment to make their own decision of what value to use as delimitation of low vs. not low risk transactions.

Refer to the following document for more information on this topic: *AN 2036—Revised Standards—Mastercard Introduces Access Control Service Risk Based Authentication and Stand-In Risk Based Authentication Service*

Smart Authentication Stand-In

The Smart Authentication Stand-In service, previously known as Stand-In RBA, is available to Issuers when being provided with EMV 3DS authentication requests. For 3DS 1.0.2 authentication requests Mastercard continues offering the Attempts Server service.

There may be instances where the Issuer's ACS services cannot be reached such as during temporary outages or connectivity issues, or when a card range or individual card is not enrolled in the Mastercard Identity Check™ Program. In such situations, Mastercard provides an authentication response on behalf of the ACS/Issuer by applying its authentication risk scoring model.

Issuers in the EEA are automatically opted-in since 17 October 2019, with opt-out option, for a purchase amount (unlimited amount during PSD2 RTS soft enforcement, and up to 30€ as from PSD2 RTS hard enforcement). In the future, Mastercard may enhance the authentication stand-in service to include Issuer TRA exemptions with a mechanism for Issuers to provide Mastercard with their maximum amount (100 EUR, 250 EUR or 500 EUR) up to which stand-in can be performed.

When the risk is low and the purchase amount does not exceed the service maximum amount (unlimited amount during PSD2 RTS soft enforcement, and up to 30€ as from PSD2 RTS hard enforcement), an approved authentication response will be returned to the Merchant or PSP with fully authenticated AAV. When the risk is high or the purchase amount exceeds the service maximum amount, or the card is not enrolled in EMV 3DS, an Attempt authentication response will be returned to the Merchant or PSP with Transaction Status = "A". In this case trying again with a 3DS 1.0 authentication is likely to be approved, which leads to higher authorization approval rates.

Issuers in the EEA have been automatically opted-in to the on-behalf AAV validation service on 17 October 2019, as only in the on-behalf validation service the Smart Authentication Stand-In generated AAV can be validated.

Issuers that have not opted out should not decline transactions that have been fully authenticated (SLI 212) by the Smart Authentication Stand-In service. They should instead

wisely use these fully authenticated transactions to drive card holder enrollment into EMV 3DS and the Mastercard ID Check program, (such as, approve some transactions and decline (with proper messaging) others if the card holder has not yet enrolled).

The fraud chargeback protection for ecommerce merchants that use SecureCode also applies for transactions using Mastercard Identity Check / EMV 3DS authentications in EEA as of 1 October 2019.

Issuers in non-regulated markets in HGEM and Switzerland will be automatically opted into the standard Stand-In Authentication service at the time of their migration to EMV 3DS and the Mastercard Identity Check™ Program.

Refer to announcements *AN 1376—Mastercard Identity Check Program and EMV 3-D Secure Version 2 (EMV 3DS) Update for Switzerland* and *AN 1396—Mastercard Identity Check Program and EMV 3-D Secure Update in High* for a complete overview of roadmap milestones and effective dates for these markets. On 1 October 2019, for Issuers in High Growth Emerging Markets and Switzerland, the Stand-In Authentication service was activated for all remaining Issuers and replaced the Attempts Server service.

Refer to the Appendix A and Appendix B for the list of concerned markets.

Refer to the following document for more information on this topic: *AN 2036—Revised Standards—Mastercard Introduces Access Control Service Risk Based Authentication and Stand-In Risk Based Authentication Service*.

AAV Validation Service

Evolving fraud patterns have highlighted the vulnerability of Issuers when transactions are processed in Stand-In without applicable validation services. Issuers continue to experience fraud losses resulting from the lack of on-behalf AAV validation services. MasterCard offers an on-behalf AAV validation service both as pre-validation (for example, the AAV is pre-validated for all authorizations sent to the Issuer authorization system) and stand-in service (for example, the AAV is validated only during Stand-In authorization processing).

If the AAV validation service is used, the Mastercard authorization stand-in stops stand-in processing, for example, not go through the remaining stand-in processing steps and finally declines the transaction, if the result code from the AAV validation service is different from "V" (AAV validation is successful).

Mastercard auto-enrolled issuers in the following countries who did not participate yet in the AAV Validation service (OBS05) and did not opt out on 13 February 2020:

- EEA issuers and issuers in Albania
- Bosnia and Herzegovina
- Kosovo
- Macedonia
- Moldova
- Montenegro

- Serbia
- Ukraine

Since 1 April 2017, Mastercard mandates AAV validation either by the Issuer (self-validation) or by Mastercard. As many Issuers use the AAV Validation Service, it is important to remind Issuers that the AAV validity period is not unlimited. It is limited to 10 business days, and 90 business days for specific MCCs. Refer to the section on Accountholder Authentication Value (AAV) Validity and Extension.

Refer to the following document for more information on this topic: *AN 1085—AAV Validation for EMV 3-D Secure*.

Chapter 8 User Experience

This chapter contains information about Mastercard recommendations for an optimal user experience with Card Not Present transactions in an EMV 3DS 2.1.0 protocol.

User Experience

Strong Customer Authentication EMV 3DS 2.1.0 User Experience Recommendations provides recommendations from Mastercard® that issuers and Access Control Servers (ACS) need to take into consideration for a good cardholder user experience as they plan their move to support EMV 3DS 2.1.0.

Strong Customer Authentication EMV 3DS 2.1.0 User Experience Recommendations can be accessed through the Publications section of Mastercard Connect™.

Chapter 9 Implementation Considerations

This document is not intended to provide information on the implementation or onboarding processes and tools.

Refer to the following documents for more information on this topic.

- *Mastercard Identity Check™ Onboarding Guide for 3-D Secure Service Providers, Operators, Issuers, and Processors* (20 September 2018)
- *Mastercard Identity Check™ Onboarding Guide for Acquirers, Merchants, and 3DS Service Providers* (20 September 2018)

Mastercard requires both the EMVCo Letter of Approval (LOA) and PCI Attestation of Compliance (AOC) for Data Security Standards or 3DS prior to the onboarding process. Merchants on the acquiring side as well as BINs or card ranges on the issuing side will be setup in Mastercard's DS by associating them respectively to their 3DS Server and ACS. 3DS Servers and ACS's receive their DS Originator ID at the end of the Mastercard Identity Check™ Compliance Testing.

It is important that Merchants and Acquirers make sure that Merchant names are unique, consistent, and as descriptive/representative as possible.

Identity Solutions Service Manager (ISSM)

The ISSM tool is available since Q4-2018. It allows Issuers or ACS's to enable and setup their card ranges, and Acquirers to enable and setup their Merchants for the Mastercard Identity Check™ Program.

On the Acquiring side, Acquirers have to manage entries in the ISSM tool for their Merchants, even in the case where the authentication process is not managed by themselves but by authentication service providers.

3D Servers should make sure that their Acquirer BIN and MID have been setup in ISSM by their Acquirer(s). If transactions are rejected for this reason, 3D Servers need to contact their Acquirer(s) to course correct.

On the Acquirer side, the Merchant name with Merchant Category Code (MCC) and country code are captured. This ensures consistency in Merchant names and allows some edits and alerts during the data entry. For example:

- Mastercard alerts the entry by different Acquirers of an existing Merchant name in a specific country.
- Mastercard alerts when an existing Merchant name is used in a specific country but by another Acquirer. The existing Merchant and the Merchant being entered should be contacted to confirm the entry.
- Mastercard alerts when an existing Merchant name is used in a different country. The existing Merchant should be contacted to confirm the entry.

Acquirers should be aware that the setup of their Merchants needs to be carefully managed to avoid potential identification issues. Acquirers are able to perform extracts of existing ISSM combinations for their Merchants. The tool aims at reaching better quality in the identification of players in the authentication value chain. It also facilitates meeting some of the PSD2 RTS requirements on SCA, such as Dynamic Linking requirements.

Issuers should only setup their card ranges in ISSM when live on their ACS (active card ranges) so that authentication requests on those can be completed successfully.

Issuers have to make sure that card ranges provided in ISSM by single entry or batch upload are for correct Primary Account Number (PAN) lengths. When potential errors are detected during single entry or batch upload, a warning is displayed by the ISSM tool. The incorrect setup of card range PAN lengths in ISSM causes transactions related to that card range to be rejected by the Mastercard Directory Server.

The access to ISSM should be granted by Issuers and Acquirers to at least two persons for backup purposes. If no one is available at the Issuer or Acquirer side, then Mastercard should be allowed to step-in to ensure business continuity.

The following amendments to the ISSM are worth mentioning in the PSD2 SCA context:

- Acquirer Exemption Indicator: allows an Acquirer to indicate which merchants can use the Acquirer TRA exemption. Availability: 28 January 2020.
- Merchant Whitelisting Name: allows an Acquirer to assign to a merchant a recognizable name used for whitelisting. Availability: 26 March 2020.
- Authentication Express Designations: allows designation of e-commerce merchants, wallet providers as well as device manufacturers participating in the Authentication Express program. It also provides participation reporting capabilities to Acquirers and Issuers. Availability: 26 March 2020.
- Merchant Name List Management: allows Acquirers and merchants to have a view on exact Merchant names and whitelisting names. Availability: 21 May 2020.

Chapter 10 Authentication Quality and Key Performance Indicators

Mastercard is updating the Data Integrity Monitoring Program with edits to monitor cardholder authentication through EMV® 3-D Secure (3DS), and fully authenticated transactions.

Force Majeure

Force Majeure is the case where exceptional circumstances lead to the unavailability of authentication/SCA capabilities (such as, the payment scheme authentication network is down for a period of time).

In such an event, Merchants want to continue accepting orders by handling such payments in off-line mode (for example, without SCA and possible delayed authorization). This is normal practice during outages impacting other payment scheme core systems such as the authorization network.

Mastercard is currently working with the EBA and national competent authorities on the understanding (identification and definition) of these cases and design of appropriate SCA fall back mechanisms (such as, off-line fall back) acknowledging that full compliance to the PSD2 RTS on SCA cannot be ensured anymore. Mastercard is also looking at introducing specific flagging of these cases, and monitoring programs to avoid misuse or abuse of these fall back mechanisms.

Authentication Quality and Key Performance Indicators

Mastercard leverages a feature of the global Data Integrity Online application on Mastercard Connect™ to send Data Integrity related alerts and notifications to customers.

The program monitors transactions to promote data quality and performs systematic validations to help ensure that customers:

- Process transactions according to Mastercard processing rules, requirements and Standards
- Adhere to product and service mandates as applicable

Registration for this application is mandatory for every ICA number and Processor ID.

The Data Integrity Monitoring Program is monitoring cardholder authentication messages using the EMV 3-D Secure protocol as well as fully authenticated 3DS transactions via new edits. Phase 1 and 2 of these new edits have been announced via:

- AN 2401—Data Integrity Monitoring Program—New Edits for EMV 3-D Secure and New Alerts and Notifications Feature: comply by date of 1 March 2020, and assessments for non-compliant customers begins 1 April 2020 for the previous month's data.
- AN 2853—Data Integrity Monitoring Program—Updates to Existing Programs and New Edits to Monitor 3DS Activity: comply by 1 September 2020, and assessments for non-compliant customers begins 1 October 2020 for the previous month's data.

The standard Data Integrity assessment structure applies, which is available in the *Data Integrity Monitoring Program* manual.

Data Integrity Monitoring is a Global program, however in several countries in Europe some KPIs are already being monitored via an Ecommerce Quality Fund (such as, approval,

Authentication Quality and Key Performance Indicators

abandonment). If that is the case, it was clearly indicated in the Data Integrity announcements which countries are excluded for a specific KPI.

Adding these additional validations helps ensure that the 3DS product is performing as designed and that consumers can enjoy both increased confidence in the security of their transactions and an efficient payment process. As a result, customers should see an improved cardholder experience with higher approval rates on card-not-present transactions and fewer chargebacks. The edits monitor Issuers and Acquirers.

In all cases, customers must be actively participating in a 3DS program and have at least 1,000 3DS transactions in a given month to be monitored.

Customers with questions about the Data Integrity Monitoring Program can contact ps_data_integrity@mastercard.com.

Additionally, Mastercard will be sending notification letters to:

- Issuers that don't support 3DS (1 nor 2)
- Issuers whose BINs are not yet registered for EMV 3DS
- Key Acquirers for their top Ecom Merchants that never send 3DS

Recipients of the notification letters should respond with a confirmation in writing that they are in compliance with the Rules or provide an action plan with a resolution date of no later than 1 July 2020.

Failure to respond may result in a non-response assessment and full assessment of the potential violation(s).

Chapter 11 Marketing, Education and Communication

Mastercard has developed a holistic Education Plan regarding PSD2/SCA requirements and Mastercard Identity Check™.

Marketing, Education and Communication

Marketing, Education and Communication

Next to numerous B2B initiatives like webinars, workshops, white papers and such, Mastercard is also playing a role in enabling stakeholders (Issuers and Merchants) to communicate to cardholders and ensure consistent messaging.

The Europe Region developed materials like a video, a Merchant FAQ, an infographic, and a communication toolkit, which are being customized for the respective markets.

Please contact your local representative for more information on this and to get access to these materials.

Chapter 12 References: What Should Customers Have Already Read on the Subject

This section lists the documentation that customers should read to understand and start preparing for the roll-out of EMV 3DS (3DS 2.0) and the Mastercard Identity Check™ Program.

Publications other than Bulletin Announcements

- *EMV 3DS - Frequently Asked Questions*
- *EMV 3DS Protocol and Core Functions Specification Version 2.2.0* (December 2018)
- *Mastercard Identity Check™ Program Guide* (19 November 2019)
- *Mastercard Identity Check™ Onboarding Guide for 3-D Secure Service Providers, Operators, Issuers, and Processors (20 September May 2018)*
- *Mastercard Identity Check™ Onboarding Guide for Acquirers, Merchants, and 3DS Service Providers* (20 September 2018)
- *Mastercard SecureCode and Mastercard Identity Check™ - Compliance and Functional Test Facility Policies Procedures*
- *SPA2 AAV for the Mastercard Identity Check™ Program*
- *Mastercard Biometric Authentication—Europe Region* (11 January 2018)
- *Consumer Device Cardholder Verification Authentication Method Requirements* (March 2018)
- *Consumer Device Cardholder Verification Authentication Method Requirements and Evaluation Program* (July 2017)
- *Mastercard Standards for Merchant Whitelisting v0.1* (May 2018)

Operations Bulletin Announcements

- (Global) Jan-16 - *Best Practices for E-Commerce—Update*
- (Global) Jan-16 - *Best Practices for Lodging, Vehicle Rental, and Cruise Lines—Update*
- (Global) Nov-16 - *Global Safety and Security Standards Roadmap*
- (Global) Nov-16 - *Announcing Mastercard Identity Check™ Authentication Program*
- (Global) Nov-16 - *EMV 3DS—Upgrading the Technology behind Mastercard SecureCode and Mastercard Identity Check™*
- (Global) Nov-16 - *Guidance on Testing Procedures for EMV 3D Secure Software*
- (Global) Nov-16 - *AAV Validation Requirement for All SecureCode and Mastercard Identity Check™ Transactions*
- (Global) Jan-17 - *Self-Validation AAV Process for SecureCode or Identity Check™ Issuers*
- (Global) Mar-17 - *Global Safety and Security Standards Roadmap—Reminder*
- (Global) Apr-17 - *AAV Validation Requirement for All SecureCode and Mastercard Identity Check™ Transactions—Clarification*
- (Global) Aug-17 - *3-D Secure 2.0 and Identity Check™ Program—Update*

Announcements

- *AN 1085—AAV Validation for EMV 3-D Secure*
- *AN 1121—Revised Standards—Credential-on-File and Recurring Payments Transactions*
- *AN 1163—Digital Safety and Security Standards Roadmap*
- *AN 1165—Identity Check™ Program and EMV 3-D Secure Version 2 (EMV 3DS) Update*
- *AN 1218—Mastercard Identity Check™ Program with EMV 3-D Secure (EMV 3DS) Rollout*
- *AN 1365—Revised Safety and Security Standards Roadmap for Germany and Liechtenstein*
- *AN 1366—Revised Safety and Security Standards Roadmap for Switzerland*
- *AN 1371—Mastercard Identity Check Program and EMV 3-D Secure Version 2 (EMV 3DS) Update for Germany and Liechtenstein*
- *AN 1376—Mastercard Identity Check™ Program and EMV 3-D Secure Version 2 (EMV 3DS) Update for Switzerland*
- *AN 1396—Mastercard Identity Check™ Program and EMV 3-D Secure Update in High Growth European Market Countries*
- *AN 1533—Revised Safety and Security Standards Roadmap for Select Countries in Central and Eastern Europe*
- *AN 1534—Digital Safety and Security Standards Roadmap for the United Kingdom, Ireland, Nordics, and Baltics*
- *AN 1544—Mastercard Identity Check™ Program and EMV 3-D Secure Version 2 (EMV 3DS) Update for Select Countries in the Europe Region*
- *AN 1630—AAV Verification Service Enhancement*
- *AN 1803—Acquirer Exemptions for Strong Customer Authentication under PSD2 and the RTS*
- *AN 1854—Guidance on Implementing Mastercard Authentication Secure Hash Algorithm —2 Certificates*
- *AN 2005—Mastercard Identity Check™ Program Update*
- *AN 2051—Contactless One-Tap PIN Request for Exemption Under PSD2 RTS Article 11*
- *AN 2113—Enhancements to AAV Validation for EMV 3- D Secure*
- *AN 2122—Introduction of Mastercard Digital Transaction Insights Service*
- *AN 2261—EMV 3DS Compliance Plan and User Experience Review Process for the CEE Countries*
- *AN 2288—Data Integrity Monitoring Program—New Edits to Monitor Use and Acceptance of Credential-On- File Indicator*
- *AN 2401—Data Integrity Monitoring Program—New Edits for EMV 3-D Secure and New Alerts and Notifications Feature*
- *AN 2479—Electronic Commerce Security Level Indicators for the Mastercard Identity*
- *AN 2509—Announcing the Prepaid Anonymous Indicator ("Anonymous Indicator")*
- *AN 2557—Revised Standards—Recurring Payment Transactions*
- *AN 2606—Enhancements to Support Contactless Tracking with Single Tap and PIN Request*
- *AN 2609—Enhancements to Support the Low-Risk Transaction Indicator for EEA Customers*

- *AN 2630—Use of Trace ID to Support PSD2 Recurring Payment Requirements*
- *AN 2639—Enhancement to SPA2 AAV Validation*
- *AN 2645—Enhancement to Low-Risk Transaction Indicator*
- *AN 2668—Handling of Authorization Response Code 65 for Contactless and Card-Not-Present Transactions*
- *AN 2684—Authentication Guide for the Europe Region*
- *AN 2714—Authentication Express—an Authentication Program Enabling Easy and Secure Multi-Lateral SCA Delegation*
- *AN 2723—Revised Standards—Europe Region PSD2 RTS Compliance for Remote Electronic Transactions*
- *AN 2724—Smart Authentication Stand-In and AAV Validation Services*
- *AN 2758—Announcing the New EMV 3DS 2.1 Mastercard Message Extension*
- *AN 2842—Clarification on the Processing of Certain EMV 3-D Secure Fields*
- *AN 2853—Data Integrity Monitoring Program—Updates to Existing Programs and New Edits to Monitor 3-DS Activity*
- *AN 2922—Updates to the Accountholder Authentication Values (AAV)*
- *AN 2962—Enhancement to Mastercard On-behalf Validation of Remote Transactions using Device Biometrics as SCA Delegation*
- *AN 2966—New Fraud Types Available in the Fraud and Loss Database for Issuers in the EEA*
- *AN 3262—Clarification on the Mastercard Adoption of EMV 3DS 2.1 with Message Extension*
- *AN 3378—Guidelines for Processing Authentications After the PSD2 SCA Effective Date for the EEA Countries*
- *AN 3440—Mastercard AAV Validation Update for Merchant Category Codes*

Appendix A Mastercard's Digital Security Roadmap

This appendix provides the Mastercard Digital Security roadmap.

Digital Security Roadmap

	Rule Change	Effective Date	Group A	Group B	Group C	Group D	Group E	Group F
Adapt authentication rules to comply with RTS	Mandate 3DS2 and ID Check Program for all Issuers	1-Apr-19	Yes	Yes	Yes	Yes	1-Sep- 19 (NAS)[9]	01-Apr-20
	Mandate 3DS2 and ID Check Program for all Acquirers/ Merchants	1-Apr-19	Yes	Yes	Yes	Yes	1-Sep-19 (NAS)[9]	01-Apr-20
	Mandate auto- and pre-enrollment	1-Jul-18	1-Oct-18	Yes	Yes (REC)[10]	Yes (REC)[10]	1-Sep-19	Yes
	Provide 3DS2 liability shift	1-Oct-19	Yes	Yes	Yes	Yes	1-Sep-19	Yes

[9] No Alternative Solution
[10] Recommended

	Rule Change	Effective Date	Group A	Group B	Group C	Group D	Group E	Group F
Enhance user experience	Mandate biometric authentication	1-Apr-19	Yes	Yes	Yes	REC[10]	1-Sep-19 (EEA)[11]	Yes
	Mandate ABU and COF flag	1-Oct-18	Acquirers for COF	Yes	31-Dec-18	31-Dec-18	Acquirers for COF	No
	Recommend merchant white listing via ACS or online banking	1-Apr-19	1-Oct-18	Yes	Yes	Yes	1-Sep-19 (EEA)[11]	No
	Recommend RBA and TRA exemptions implementation vs. usage	Immediately	Yes	Yes	Yes	Yes	1-Sep-19 (EEA)[11]	Yes (RBA)[12]
Reduce fraud, increase approval rates	Mandate issuer must be able to require SCA	1-Apr-19	Yes	Yes	Yes	No	1-Sep-19 (EEA)[11]	No
	Mandate Transaction Alerts	1-Jul-18	Live in UK	Yes	31-Dec-19	31-Dec-19	1-Sep-19 (REC)[10]	No
	Recommend Decision Intelligence	15-Jan-18	No	Yes	Yes (NOO)[13]	Yes (NOO)[13]	No	No
			Denmark	**Andorra**	**Germany**	**Switzerland**	**Albania**	**Armenia**

[11] In EEA
[12] Risk-Based Authentication
[13] No Opt-Out

	Rule Change	Effective Date	Group A	Group B	Group C	Group D	Group E	Group F
			Estonia	Belgium	Liechtenst		Austria	Azerbaijan
			Finland	France			Bosnia & Her	Belarus
			Iceland	Gibraltar			Bulgaria	Georgia
			Ireland	Italy			Croatia	Kazakhstan
			Latvia	Luxembourg			Cyprus	Kyrgyzstan
			Lithuania	Monaco			Czech Rep.	Moldova
			Norway	Netherlands			Greece	Russia
			Sweden	Portugal			Hungary	Tajikistan
			UK	SanMarino			Israel	Turkey
				Spain			Kosovo	Turkmenist.
				VaticanCity			Macedonia	Ukraine
							Malta	Uzbekistan
							Montenegro	
							Poland	
							Romania	
							Serbia	
							Slovakia	
							Slovenia	

Appendix B Reference Announcements for all Countries in Europe

This appendix provides a list of announcements that are related to the roll-out of EMV 3DS (3DS 2.0) and the Mastercard Identity Check™ Program.

Reference Announcements for all Countries in Europe

Reference Announcements for all Countries in Europe

Country Name EEA Over seas	If EEA, Country	Division (Long)	Division (short)	If EEA, Currency	
Aland Islands[14]	ALA-248	UK and Ireland, Nordics and Baltics	UKINB	EUR-978	
Albania		Central Eastern Europe	CEE		1533
Andorra		Western Europe	WE		1163
Armenia		High Growth Emerging Markets	HGEM		1396
Austria	AUT-040	Central Eastern Europe	CEE	EUR-978	1533
Azerbaijan		High Growth Emerging Markets	HGEM		1396
Belarus		High Growth Emerging Markets	HGEM		1396
Belgium	BEL-056	Western Europe	WE	EUR-978	1163
Bosnia and Herzegovina		Central Eastern Europe	CEE		1533
Bulgaria	BGR-100	Central Eastern Europe	CEE	BGN-975[15]	1533
Croatia	HRV-191	Central Eastern Europe	CEE	HRK-191[15]	1533
Cyprus	CYP-196	Central Eastern Europe	CEE	EUR-978	1533
Czech Republic	CZE-203	Central Eastern Europe	CEE	CZK-203[15]	1533

[14] EEA Overseas
[15] non EUR

Reference Announcements for all Countries in Europe

Country Name EEA Over seas	If EEA, Country	Division (Long)	Division (short)	If EEA, Currency	
Denmark	DNK-208	UK and Ireland, Nordics and Baltics	UKINB	DKK-208[15]	1534
Estonia	EST-233	UK and Ireland, Nordics and Baltics	UKINB	EUR-978	1534
Finland	FIN-246	UK and Ireland, Nordics and Baltics	UKINB	EUR-978	1534
France	FRA-250	Western Europe	WE	EUR-978	1163
French Guiana[14]	GUF-254	Western Europe	WE	EUR-978	
Georgia		High Growth Emerging Markets	HGEM		1396
Germany	DEU-276	Germany and Switzerland	GandS	EUR-978	1365
Gibraltar	GIB-292	Western Europe	WE	GIP-292	1163
Greece	GRC-300	Central Eastern Europe	CEE	EUR-978	1533
Guadeloupe[14]	GLP-312	Western Europe	WE	EUR-978	
Hungary	HUN-348	Central Eastern Europe	CEE	HUF-348[15]	1533
Iceland	ISL-352	UK and Ireland, Nordics and Baltics	UKINB	ISK-352[15]	1534
Ireland	IRL-372	UK and Ireland, Nordics and Baltics	UKINB	EUR-978	1534
Israel		Central Eastern Europe	CEE		1533
Italy	ITA-380	Western Europe	WE	EUR-978	1163
Kazakhstan		High Growth Emerging Markets	HGEM		1396

Reference Announcements for all Countries in Europe

Country Name EEA Over seas	If EEA, Country	Division (Long)	Division (short)	If EEA, Currency	
Kosovo		Central Eastern Europe	CEE		1533
Kyrgyzstan		High Growth Emerging Markets	HGEM		1396
Latvia	LVA-428	UK and Ireland, Nordics and Baltics	UKINB	EUR-428	1534
Liechtenstein	LIE-438	Germany and Switzerland	GandS	CHF-756[15]	1365
Lithuania	LTU440	UK and Ireland, Nordics and Baltics	UKINB	EUR-978	1534
Luxembourg	LUX-442	Western Europe	WE	EUR-978	1163
Macedonia		Central Eastern Europe	CEE		1533
Malta	MLT-470	Central Eastern Europe	CEE	EUR-978	1533
Martinique[14]	MTQ-474	Western Europe	WE	EUR-978	
Mayotte[14]	MYT-175	Western Europe	WE	EUR-978	
Moldova		High Growth Emerging Markets	HGEM		1396
Monaco		Western Europe	WE		1163
Montenegro		Central Eastern Europe	CEE		1533
Netherlands	NLD-528	Western Europe	WE	EUR-978	1163
Norway	NOR-578	UK and Ireland, Nordics and Baltics	UKINB	NOK-578[15]	1534
Poland	POL-616	Central Eastern Europe	CEE	PLN-985[15]	1533

Reference Announcements for all Countries in Europe

Country Name EEA Over seas	If EEA, Country	Division (Long)	Division (short)	If EEA, Currency	
Portugal	PRT-620	Western Europe	WE	EUR-978	1163
Reunion[14]	REU-638	Western Europe	WE	EUR-978	
Romania	ROU-642	Central Eastern Europe	CEE	RON-946[15]	1533
Russia		High Growth Emerging Markets	HGEM		1396
San Marino		Western Europe	WE		1163
Serbia		Central Eastern Europe	CEE		1533
Slovakia	SVK-703	Central Eastern Europe	CEE	EUR-978	1533
Slovenia	SVN-705	Central Eastern Europe	CEE	EUR-978	1533
Spain	ESP-724	Western Europe	WE	EUR-978	1163
Svalbard and Jan Mayen[14]	SJM-744	UK and Ireland, Nordics and Baltics	UKINB	NOK-578	
Sweden	SWE-752	UK and Ireland, Nordics and Baltics	UKINB	SEK-752[15]	1534
Switzerland		Germany and Switzerland	GandS		1365
Tajikistan		High Growth Emerging Markets	HGEM		1396
Turkey		High Growth Emerging Markets	HGEM		1396
Turkmenistan		High Growth Emerging Markets	HGEM		1396
Ukraine		High Growth Emerging Markets	HGEM		1396

Reference Announcements for all Countries in Europe

Country Name EEA Over seas	If EEA, Country	Division (Long)	Division (short)	If EEA, Currency	
United Kingdom	GBR-826	UK and Ireland, Nordics and Baltics	UKINB	GBP-826[15]	1534
Uzbekistan		High Growth Emerging Markets	HGEM		1396
Vatican City		Western Europe	WE		1163

Appendix C List of Acronyms

The appendix provides a list of acronyms used throughout this manual and their descriptions.

Acronyms

The following acronyms are used throughout this manual.

Acronym	Name
3DS	Three Domain Secure
3RI	3DS Requestor Initiated (Non-payment and Payment)
AAV	Accountholder Authentication Code
ABU	Automatic Billing Updater
ACS	Access Control Server
AReq	Authentication Request
ARes	Authentication Response
AuthE	Authentication
AuthO	Authorization
B2B	Business-to-Business
BAU	Business As Usual
BIN	Bank Identification Number
BPS	Basis Points
BRN	Banknet Reference Number
CAB	Card Acceptor Business
CDCVM	Consumer Device Cardholder Verification Method
CIS	Customer Interface Specifications
CIT	Cardholder or consumer Initiated Transaction
CNP	Card Not Present
COF	Card-On-File
CP	Card Present
CReq	Challenge Request
CRes	Challenge Response
CVM	Cardholder Verification Method
DS	Directory Server
DTI	Digital Transaction Insights
EBA	European Banking Authority

Acronym	Name
ECI	Electronic Commerce Indicator
EEA	European Economic Area
EMV	Europay Mastercard VISA
GDPR	General Data Privacy Regulation
GDS	Global Distribution System
HTML	Hypertext Markup Language
IAV	Issuer Authentication Value
ICA	Interbank Card Association
ICCP	
IPM	Integrated Product Messages
KBA	Knowledge-Based Authentication
KPI	Key Performance Indicator
LVP	Low-Value Payments
MCC	Merchant Category Code
MDES	Mastercard Digital Enablement Service
MIT	Merchant-Initiated Transactions
MLRMP	Maestro Low Merchant Risk Program
MOTO	Mail Order Telephone Order
MPE	Member Parameter Extract
MRPP	Maestro Recurring Payment Program
MUPP	Maestro Utility Payment Program
NCA	National Competent Authority
OBS	On-Behalf Service
OOB	Out Of Band
OTP	One Time Password
PAN	Primary Account Number
PKE	PAN Key Entry
PReq	Preparation Request
PRes	Preparation Response
PSD	Payment Services Directive
PSP	Payment Service Provider

Acronym	Name
RBA	Risk-Based Authentication (also known as "passive" or "silent" authentication)
RReq	Results Request
RRes	Results Response
RTS	Regulatory Technical Standards
SAFE	System to Avoid Fraud Effectively
SCA	Strong Customer Authentication
SLI	Security Level Indicator
SPA	Secure Payment Application
TCC	Transaction Category Code
TRA	Transaction Risk Analysis
UCAF	Universal Cardholder Authentication Field
UI	User Interface
UX	User Experience
VCN	Virtual Card Number

Appendix D EMV 3DS Fields

This appendix provides EMV 3DS fields.

Clarifications on EMV 3DS Conditional Fields

There are a number of conditional fields that have been defined by the EMVCo.

Among them, the following fields are considered key ones and are conditional on no market restriction.

- Cardholder Information:
  - Name
  - Email address
  - Home phone number
  - Mobile phone number
  - Billing address
  - Shipping address
- Browser Information:
  - IP Address

To improve the overall cardholder experience by avoiding unnecessary challenges and increase the approval rate of ecommerce transactions, the following apply:

- Merchants must send conditional fields in EMV 3DS messages in accordance with the applicable data protection law. In the European Economic Area (EEA), merchants must determine a valid legal ground for such data processing activity under the General Data Protection Regulation (GDPR). Mastercard considers that such legal ground may be, for instance, the legitimate interest of the merchant and/or issuer to prevent fraud or the legal obligation of the issuer to authenticate the cardholder under Payment Services Directive 2 (PSD2), having additional regard to other applicable GDPR safeguards, such as providing sufficient notice and opt-out.
- The provision of these conditional fields may improve the authorization approval rate related to these ecommerce transactions as confirmed by the markets. ACSs may achieve a better risk assessment leading to more risk-based authenticated and less challenged transactions.
- ACSs must not decline EMV 3DS messages when one or more of these conditional fields are absent. ACSs in this case must modify their authentication platform to not systematically decline EMV 3DS messages with absent or blank-filled conditional fields. These modifications should be put in place immediately and in EEA countries before the PSD2 Regulatory Technical Standards (RTS) effective date 14 September 2019.

Communicating EMV 3DS Failures to Cardholders

As a reminder, authentication error messages (especially card not enrolled) should be sent by the ACS and displayed by the 3D Server/Merchant via the following fields:

- CardholderInfo for frictionless
- ChallengeInfoText for challenge flow

As the above-mentioned fields are optional, Mastercard recommends to display the information to the end consumer when the fields are populated.

For cardholders that are not registered, the following recommendations apply:

- The ACS should apply RBA for these instead of declining, unless SCA is required.
- Merchants should try again with 3DS 1.0 when they receive an attempt AAV or send straight to authorization (until 10 October 2019, no attempt AAV will be provided for EMV 3DS).

Handling of Special Characters

Special characters are supported for all fields. The following paragraphs apply to the one field does not support special characters: the card holder name.

For the card holder name, Mastercard is reminding all stakeholders that the only special characters allowed in EMVCo 3DS fields are those defined in the EMV Book 4 - Appendix B. The allowed character set includes each of the lowercase and uppercase. The values that are allowed are in the range from binary 0010 0000 - hexadecimal 20 (decimal 32) to binary 0111 1110 hexadecimal 7E (decimal 126) that constitute the Common Character Set.

All other special characters in the range from binary 1000 0000 - hexadecimal 80 (decimal 128) to binary 1111 1110 - hexadecimal FE (decimal 254) will cause the EMV 3DS authentication message to be rejected by the Mastercard Directory Server. These are non-common character sets defined by the ISO/IEC 8859 parts (1-16) that have been defined to cover all languages based on language root: Latin, Cyrillic, Arabic, Greek, Hebrew, and so on. Characters that will be rejected include those using diacritical marks (such as, é, ä) or symbols (such as, ß, ç). Again, the limitation on the usage of special characters applies to the card holder name only.

Appendix E Travel Sector Use Cases

This appendix addresses the most common use cases within the travel sector.

About Travel Sector Use Cases

Payments for travel services include transportation purchases (such as, airline, train or other transportation tickets), accommodations (such as, hotel bookings) and car rentals. Purchases can be made directly through a Travel Supplier such as an airline or indirectly via Travel Agents or third parties. Payments may also be completed at the time of the booking or delayed (for example, reserve now and pay later).

Audience

The Travel Sector Use Cases section is targeted to the following audiences:

- Travel, Transportation and Accommodation Suppliers (such as, airlines, hotels, car rentals, cruise companies)
- Travel Agents (such as, Online Travel Agents, brick-and-mortar Travel Agents, Travel Management Companies, Tour Operators)
- Payment Service Providers serving the travel industry (such as, Issuers, Acquirers, PSPs, EMV 3DS MPI providers)
- Other Third Party Service Providers serving the travel industry (such as, Global Distribution Systems (GDS), Data Aggregators, Channel Managers, Technology and Infrastructure providers)
- Travel Industry Bodies

Terms

The following terms are used in this Appendix E, Travel Sector Use Cases.

- Merchant of Record = The Merchant that sells the good and services to the consumer needs to be reflected in the authentication and authorization. As much as possible, the Merchant name must be consistent between authentication and authorization
- Travel Supplier = An entity supplying a travel service (such as, airlines, hotels, car rentals)
- Travel Agent = An entity managing bookings on behalf of Travel Suppliers, either online or offline (such as, Online Travel Agencies, Travel Management Companies, Tour Operators, Wholesale providers)
- Service Provider = An entity providing services to the Travel Providers and/or Suppliers (such as, Data Aggregators, Technology Providers, Channel Managers).
- GDS = Global Distribution System
- OTA = Online Travel Agent
- PSS = Passenger Service System
- CRS = Central Reservation System
- Lodged Cards = A commercial card that is lodged with a company-approved third party within an access-controlled environment, such as a corporate travel company that books travel and hotels on behalf of the company via secure dedicated payment process and protocol.

- Virtual Card Numbers (VCNs) = VCNs are generated over dedicated payment processes and protocols for pre-defined transactions as established by the corporate. The generation of VCNs occurs within a secure and controlled environment, typically via a secure two-factor-authentication process or via APIs. Virtual Cards come with a large set of controls such as transaction value, validity period, Merchant type and currency.

Authentication for Direct Sales

Direct Sales refers to those bookings made directly by a cardholder with the Travel Supplier operating the service (such as, airline, hotel) while the cardholder is IN SESSION.

According to PSD2 guidelines, SCA is required when booking transactions are made online by the cardholder while the cardholder is available behind his device to authenticate unless an exemption applies or unless the transaction is out-of-scope.

Direct Sales includes purchases made:

- Online through a Travel Supplier's website (such as, airline website, hotel website);
- Online through a Central Reservations System (such as, brand.com sites)
- In-person, such as at the airport, at check-in or in-flight, or onsite at the property; and
- Other Travel Supplier's channels including over the phone (such as, MOTO)

Direct Sales: Transactions Made Through Ecommerce Channels

Direct Sales transactions can be initiated through various systems or environments.

Online Through a Travel Supplier Website

Transactions conducted through Ecommerce Channels are in scope of PSD2 and must be processed as ecommerce. The Cardholder makes a booking for a travel service (such as, airline or train ticket, accommodation or car rental) on the Travel Supplier's website or mobile app.

In this instance, the Travel Supplier must authenticate the Cardholder at the time the booking is made, while the Cardholder is in session. Certain transactions may be eligible for an Acquirer or Issuer exemption.

When airlines, hotels are organizing the reservation/booking and payment of their travel services, they are the Merchant of Record (MoR) during the transaction and need to be identified as such in authentication and authorization.

Within the ecommerce channel, there are multiple payment scenarios:

- Pay Now:
  - The Cardholder completes the payment at the time of the booking
  - The Travel Supplier is identified as the MoR and processes the payment as a regular one-time ecommerce transaction via their PSP or Acquirer
  - Under PSD2 guidelines, SCA is conducted unless an exemption applies
  - If an exemption is applied (such as, Transaction Risk Analysis), authentication may be skipped and the transaction may be sent directly to authorization

  - The payment transaction is processed by the Travel Supplier upon completion of the booking

Example Use Case: Cardholder books an airline ticket using the airline's website.

- Reserve Now, Pay Later:
  - The traveler reserves the service, but the payment is not completed at the time of the booking
  - The Travel Supplier (such as, hotel) is still considered the MoR under this scenario
  - The Travel Supplier provides authorization within 90 days after authentication
  - If authorization happens later than 90 days it should be handled as a MIT (with SCA being required for the online reservation)
  - If multiple payments are expected between the Cardholder and the Merchant, then a Merchant Initiated Transaction (MIT) agreement may be deployed. Under this scenario, the Merchant has the option to initiate a MIT at the time of booking.

Example: MIT Use Case: Hotel reservation or car rental booking where a reservation is made, but no payment is collected upfront. Vacation package where a deposit is collected upfront followed by subsequent payments. In most cases, the transaction process would proceed as follows:

1. The Cardholder reserves the travel service with their card and authentication is completed. This reservation explicitly shows the conditions of the MIT agreement or mandate at time of authentication. The Travel Supplier uses the customer payment card as a 'guarantee' for the service, for example as a means to apply any no-show fees.
2. The MIT agreement authentication needs to be authorized by the Travel Supplier. Amount should be as reflected in the MIT agreement.
3. At the start of the service (such as, checking in at hotel or pick-up at car rental location) the Travel Supplier pre-authorizes the customer card with an agreed amount, based on the Travel Supplier's T&Cs.
4. Upon completion of the service, payments are processed based on the services consumed by the Cardholder (such as, length of stay at the hotel).
5. In case of no-shows: The amount will be charged as agreed in the MIT.

Online Through a Central Reservations System (Same Principles as with Travel Agent)
The Cardholder makes a booking for a travel service (such as, accommodation or car rental) through a Central Reservations System (for example, hotelbrand.com site).

There are two main scenarios that can apply:

- Central Reservations System is MoR:
  - The Cardholder accesses an Ecommerce Channel (website, mobile app) and books a service
  - The Central Reservations System manages the reservation and takes payment for the services
  - Under PSD2, SCA is conducted unless and exemption applies
  - The Central Reservations System would have to apply SCA and use their own EMV 3DS MPI at the time of booking when the customer is IN SESSION

  - The Central Reservations System processes the transactions on the Cardholder's card as a standard, one-time ecommerce transaction and passes on the fully authenticated AAV in authorization
  - The Central Reservations System remits the funds to the entity providing the service
- Central Reservations System pass through model:
  - Traveler accesses an Ecommerce Channel (website, mobile app) and books a service
  - The Central Reservations System organizes the reservation and passes the traveler's payment details to the entity providing the service
  - The Central Reservations System would have to apply SCA and use their own EMV 3DS MPI at the time of booking when the customer is IN SESSION
  - Once the reservation is confirmed and authentication has been carried, the Central Reservation System would send the Cardholder's card details (PAN, Expiry Date and CVC) as well as the authentication and AAV information to the entity providing the service and processing the payment.
  - For those entities processing transactions as MOTO or PAN Key Entry, refer to the sections Mail Order/Telephone Order (MOTO) and Manual Card Entry in this document.
- There might be scenarios where the Central Reservations System would redirect Travelers to the booking page of the entity providing the service and processing the payment. As such, this entity will be considered MoR and would have to authenticate following the steps indicated in section Online through a Travel Supplier Website of this document.

Direct Sales: Transactions Made In-person/Physical Channel

Purchases made in person for travel or ancillary services from a Travel Supplier may still be in scope of PSD2 and need to be evaluated on a case by case basis in order to determine the appropriate authentication mechanism.

- At the airport, during check-in or at boarding
  Example: Airline ticket purchases, upgrades, fees for excess baggage or ancillary charges)
- In-flight, on the train, and so forth
  Example: Food and beverages, duty-free goods, or other ancillary services purchased on board
- Transactions made in person (for example, hotel accommodation or car rental) are processed as Card Present. In this physical environment, CHIP/PIN should be enabled at the POS terminal.
- It is critical that transactions are coded correctly in authorization and clearing. For example, a payment cannot be accepted as ecommerce and then converted to a MOTO transaction in clearing.

Direct Sales: Transactions Made via Other Channels while Cardholder is In-session

Payments for travel or ancillary services through a call center are classified as a Mail Order/ Telephone Order (MOTO). These are payments made via a call center where the Cardholder provides card details to an Agent that processes the payment.

The Acquirer/Travel Supplier is responsible for flagging MOTO transactions correctly.

Authentication for Indirect Sales

Indirect Sales refers to those bookings made via a Travel Agent that is not the Merchant operating the service.

In the indirect flow Acquirer exemptions can only be applied for authentication based on the agreement between Merchant of Record and Acquirer. Any exemptions should be notified by the Merchant of Record and/or Acquirer to the Travel Agent. Otherwise, the Travel Agent may not apply any exemptions. It is recommended that for indirect sales, Acquirer exemptions are applied through authentication and not through authorization:

Exemptions should be used cautiously when there is a delay between authentication and authorization. If an Issuer (soft) declines an exemption, the risk is that authentication is not possible anymore because cardholder is already out of session.

Indirect Online Sales via Travel Agent

When customers purchase travel services or make reservations using a Travel Agent there is no direct interaction between the customer and the end Travel Supplier (for example, airline, hotel or car rental agency).

Travel Agents can be connected to a Global Distribution System (GDS), to a Service Provider, to Travel Suppliers or to a combination of these.

Currently, varied authentication practices are in use under the Indirect Sales model. For transactions booked online, either the Travel Agent, the GDS or the Service Provider is responsible for authenticating the cardholder.

Indirect Online Sales via Travel Agent using Global Distribution System or Service Providers

There are different options depending on the Merchant of record.

Options if Travel Agent is MoR

If the Travel Agent is the MoR, the Travel Agent will complete the purchase by enabling two transactions. The traveler pays the Travel Agent (payment flow 1) and the Travel Agent settles the payments with the Travel Supplier (payment flow 2). The example illustrates the use of VCN for payment flow 2.

- Initial Transaction (Treated as e-commerce and SCA applied)
  - Traveler initiates booking with the Travel Agent
  - Travel Agent applies SCA using their own EMV 3DS MPI at the time of booking when the customer is IN SESSION and passes on the fully authenticated AAV in authorization
  - Travel Agent processes the transaction on the customer's card as a standard, one-time E-commerce transaction in authorization
- Secondary Transaction (Virtual Card Number Transaction Treated as MOTO or Secure Corporate Payment):
  - Travel Agent sends VCN details to the GDS or the Service Provider. The VCN can be treated as MOTO or Secure Corporate Payment.

  - If the VCN payment is classified as MOTO, it is out of scope for PSD2. Proper MOTO flags should be used (see Authentication Guide).
  - For Secure Corporate Payments, flags are provided in authentication as well as authorization.
- The GDS or the Service Provider passes the VCN details to the Travel Supplier.

  NOTE: For those airline transactions that are authorized by the GDS on behalf of the airline, the GDS would need to apply the corresponding flags in the authentication and/or authorization as appropriate.

- If GDS/Service Providers or Travel Suppliers are in doubt on whether the card details received belong to an exempt product, it's advised to apply Strong Customer Authentication.

Options if Travel Supplier is MoR (Pass-through Agent Model)

If the Travel Supplier is designated the MoR, and the booking is handled by a Travel Agent, the authentication should be made while in session.

The Travel Agent authenticates the transaction and sends the authentication details and the traveler's card details to the GDS, the Service Provider or the Travel Supplier as appropriate. If the GDS or the Service Provider is the recipient of this data, they forward it to the Travel Supplier.

NOTE: For those airline transactions that are authorized by the GDS on behalf of the airlines, the GDS uses, in the authorization fields, their own Acquirer BIN and MID and the authentication details received by the Travel Agent. For more information see sections Merchant Location and Merchant Identification.

There might be some GDS or Service Providers that have their own EMV 3DS MPI and use it to authenticate certain transactions. If any of these entities is performing the authentication, they have to use their own Acquirer BIN and MID in the authentication fields. See sections Merchant Location and Merchant Identification for more information.

Indirect Online Sales via Travel Agent using Direct Connection to Travel Suppliers

There are different options depending on the Merchant of record.

Options if Travel Agent is MoR

If the Travel Agent is the MoR, the Travel Agent completes the purchase by enabling two transactions.

The traveler pays the Travel Agent (payment flow 1) and the Travel Agent settles the payments with the Travel Supplier (payment flow 2). The following example illustrates the use of VCN for payment flow 2.

- Initial Transaction (Treated as ecommerce and SCA applied)
  - Traveler initiates booking with Travel Agent
  - Travel Agent applies SCA using their own EMV 3DS MPI at the time of booking when the customer is IN SESSION and passes on the fully authenticated AAV in authorization

  - Travel Agent processes the transaction on the customer's card as a standard, one-time e-commerce transaction in authorization
- Secondary Transaction (Virtual Card Number Transaction Treated as MOTO or Secure Corporate Payment):
  - Travel Agent sends their payment details to the Travel Supplier, typically a VCN. When VCN is used as payment method, it can be treated as MOTO or Secure Corporate Payment.
    - If the VCN payment is classified as MOTO, it is out of scope for PSD2. Proper MOTO flags should be used.
    - For Secure Corporate Payments, flags are provided in authentication as well as authorization.
  - The Travel Supplier would then process the payment and would need to apply the corresponding flags in the authentication and/or authorization as appropriate.
  - If Travel Suppliers are in doubt on whether the card details received belong to an exempt product, it's advised that Travel Suppliers apply Strong Customer Authentication.

Options if Travel Supplier is MoR (Pass-through Agent Model)
The booking is handled by the Travel Agent but the Travel Supplier is the MoR.

- Traveler initiates booking with Travel Agent
- Travel Agent applies SCA using their own EMV 3DS MPI at the time of booking when the customer is IN SESSION and passes the authentication and the traveler's card details to the Travel Supplier. The Travel Agent authenticates the transaction using their own Acquirer BIN (or one provided by their Service Provider) and MID. For more information see sections Merchant Location and Merchant Identification.

Recommendations
Mastercard recommends the following for an optimal handling of indirect online sales.

- The Travel Agent should apply SCA on behalf of the Merchant/ Acquirer (a formal agreement between the two parties may be required)
- This requires Travel Agents to enable a booking tool that supports EMV 3DS as well as the Merchant/Acquirer to outsource SCA to the booking tool provider.
- This may also require additional logic to be built so that the booking tool can identify and use the Acquirer BIN and Merchant ID registered by the Acquirer of the Merchant during authentication.
- In the event of authorization being done by a GDS, the Travel Agent should share the authentication details with the GDS to allow a standard CNP authorization to be initiated. Authentication details should include protocol version, DS Transaction ID, SLI, exemptions requested and the AAV.
- MID and Acquirer BIN used as identifiers in the authentication must have been registered with the Mastercard ID Check Authentication network, if not authentication is rejected. These identifiers do not need to be repeated in the authorization or clearing. Acquirers must make efforts to have a consistent use of Merchant Name in authentication and authorization.

- If the Acquirer relationship is not known at the time of booking, it is not be possible to apply an Acquirer Exemption.

Indirect Offline Sales via Travel Agent

In the offline environment, the customer makes a booking through a Travel Agent at a physical location (such as, store).

This a face to face transaction (for example, Card Present), which does not require authentication.

Indirect Online Sales of Ancillary Services via Travel Supplier

It is common in the Travel Industry for Travel Suppliers to sell additional services to their customers that are provided by different suppliers (such as, travel insurance, bus tickets).

In this case the Travel Supplier is acting as the Travel Agent, and section Indirect Online Sales via Travel Agent using Direct Connection to Travel Suppliers applies, either using the pass-through model or acting as the Merchant of Record.

Authentication for Secure Corporate Payment Transactions

Refer to the section Secure Corporate Payments in this manual for details on the authentication guidelines related to this topic.

The table below outlines the recommended approach for authenticating and authorizing the transactions under specific Travel Sector Use Cases.

Type	Section	Core Use Case	Merchant of Record (MoR)	Authentication	Authorization
Direct Sales	Direct Sales: Transactions Made Through Ecommerce Channels (in case of Central Reservation System, the Travel Agent case applies - see below)	Transactions made through Ecommerce Channels	Travel Supplier (authentication) MerchantName = (authorization) DE43 SF1 = TSPName	Travel Supplier - SCA unless an exemption applies. If exemption, going straight to authorization is allowed. The AAV validity is 90 days. For MIT: • SCA at agreement setup	Travel Supplier - regular ecom or MIT if payment after AAV validity period or multiple payments are involved. For MIT: • Subsequent: Trace ID (DE48 SE63) of SCA and • MIT flag on (DE 48 SE 22 SF 1=01)
	Direct Sales: Transactions Made In-person / Physical Channel	Transactions made in-person / physical channel		Card present/ physical environment with CHIP & PIN at POS. PAN Key Entry ad interim during infrastructure upgrade.	As Merchants might be in process of making terminal compliant, it is acceptable not to decline manual PAN Key Entry.
	Direct Sales: Transactions Made via Other Channels while Cardholder is In-session	Transactions made via other Channels while Cardholder is in-session		Travel Supplier - MOTO	Travel Supplier - MOTO

Type	Section	Core Use Case	Merchant of Record (MoR)	Authentication	Authorization
Indirect Sales	Indirect Online Sales via Travel Agent (using GDS or Service Provider)	Online Sales - Travel Agent using GDS or Service Provider. Travel Agent is the MoR and makes a secondary payment to the Travel Supplier.	1. Travel Agent (first transaction - B2C) 2. Travel Supplier (second transaction - B2B) For 1, (authentication) MerchantName = (authorization) DE43 SF1 = TAName	1. Travel Agent – SCA (See Direct Sales: Transactions Made Through Ecommerce Channels. 2. GDS - SCA on the Travel Agent VCN (probably Secure Corporate Payment exemption).	Travel Agent - regular ecom (See Direct Sales: Transactions Made Through Ecommerce Channels. GDS processes the VCN directly with the card scheme.

Type	Section	Core Use Case	Merchant of Record (MoR)	Authentication	Authorization
		Online Sales - Travel Agent using GDS or Service Provider Travel Supplier is the MoR (passthrough agent model) with customer's card.	Travel Supplier (authentication) MerchantName = (authorization) DE 43 SF 1 = TSName If multi-Merchant booking, First = TAName Subsequent = TAName*TSName	Travel Agent - SCA (See Direct Sales: Transactions Made Through Ecommerce Channels). GDS - gets authentication information from the Travel Agent. TA Acquirer BIN and MID (different from MoR Acquirer BIN and MID). If the Travel Agent is unable to authenticate the transaction, the GDS/Service Provider may perform the authentication with their own EMV 3DS-Server. GDS / Service Provider Acquirer BIN and MID (different from MoR Acquirer BIN and MID).	GDS - regular ecom (See Direct Sales: Transactions Made Through Ecommerce Channels). GDS processes transaction directly with the card scheme on the GDS/ Acquirer BIN and with a Merchant code (instead of a MID) as it may be unknown which Acquirer the Travel Supplier is working with. In the authorization, the GDS will use the authentication details passed by the Travel Agent. If the GDS authenticates the transaction, the GDS will use this authentication data for the authorization.

Type	Section	Core Use Case	Merchant of Record (MoR)	Authentication	Authorization
	Indirect Online Sales via Travel Agent using Direct Connection to Travel Suppliers	Online Sales - Travel Agent using direct connection to the Travel Supplier. Travel Supplier is the MoR (passthrough agent model) with customer's card.		Travel Agent - SCA (See Direct Sales: Transactions Made Through Ecommerce Channels). Travel Supplier - gets authentication information from the Travel Agent. TA Acquirer BIN and MID (different from MoR Acquirer BIN and MID).	Travel Service Provider - regular ecom (See Direct Sales: Transactions Made Through Ecommerce Channels). Travel Service Provider processes the transaction with their PSP and inserts the authentication details provided by the Travel Agent.
		Online Sales - Travel Agent using direct connection to the Travel Supplier. Travel Agent is the MoR and makes a secondary payment to the Travel Supplier.		1. Travel Agent - SCA (See Direct Sales: Transactions Made Through Ecommerce Channels). 2. Travel Supplier - SCA on the Travel Agent VCN (probably Secure Corporate Payment exemption).	Travel Agent - regular ecom (See Direct Sales: Transactions Made Through Ecommerce Channels). Travel Supplier processes the VCN with their PSP.

Type	Section	Core Use Case	Merchant of Record (MoR)	Authentication	Authorization
	Indirect Online Sales of Ancillary Services via Travel Supplier (in this case, the Travel Supplier is acting as the Travel Agent, so section Indirect Online Sales via Travel Agent using Direct Connection to Travel Suppliers applies - see above)				

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

Information Available Online

Mastercard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on Mastercard Connect™. Go to Publications Support for centralized information.